SIAM J. COMPUT.
Vol. 40, No. 3, pp. 848–877

ENTANGLED GAMES ARE HARD TO APPROXIMATE*

JULIA KEMPE†, HIROTADA KOBAYASHI‡, KEIJI MATSUMOTO‡, BEN TONER§, AND THOMAS VIDICK¶

Abstract. We establish the first hardness results for the problem of computing the value of one-round games played by a verifier and a team of provers who can share quantum entanglement. In particular, we show that it is NP-hard to approximate within an inverse polynomial the value of a one-round game with (i) a quantum verifier and two entangled provers or (ii) a classical verifier and three entangled provers. Previously it was not even known if computing the value exactly is NP-hard. We also describe a mathematical conjecture, which, if true, would imply hardness of approximation of entangled-prover games to within a constant. Using our techniques we also show that every language in PSPACE has a two-prover one-round interactive proof system with perfect completeness and soundness $1 - 1/\operatorname{poly}$ even against entangled provers. We start our proof by describing two ways to modify classical multiprover games to make them resistant to entangled provers. We then show that a strategy for the modified game that uses entanglement can be "rounded" to one that does not. The results then follow from classical inapproximability bounds. Our work implies that, unless P = NP, the values of entangled-prover games cannot be computed by semidefinite programs that are polynomial in the size of the verifier's system, a method that has been successful for more restricted quantum games.

Key words. interactive proofs, quantum computing, entanglement, almost-commuting matrices

AMS subject classifications. 81P68, 68Q10

DOI. 10.1137/090751293

1. Introduction.

Multiprover games have played a tremendous role in theoretical computer science over the last two decades. In this setting, several provers, who are not allowed to communicate with each other during the game, exchange messages with a verifier according to a prescribed protocol and try to convince him to accept. The *value* of a game is the maximum probability with which the provers can achieve this, averaged over all the verifier's questions possibly over the shared randomness of the provers. The Cook–Levin theorem implies that it is NP-complete to compute the

*Received by the editors March 2, 2009; accepted for publication (in revised form) October 1, 2010; published electronically June 23, 2011.
http://www.siam.org/journals/sicomp/40-3/75129.html

†School of Computer Science, Tel Aviv University, Tel Aviv, Israel (kempe@post.tau.ac.il). This work was partly done while this author was at LRI, Univ. de Paris-Sud, Orsay. This author's work was partially supported by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as contract 015848, by an Alon Fellowship of the Israeli Higher Council of Academic Research, by a grant of the Israeli Science Foundation, by an ERC Starting Researcher grant, and by a grant from the Wolfson Family Charitable Trust. Support by Michel Cukierman is also gratefully acknowledged.

‡Principles of Informatics Research Division, National Institute of Informatics, Tokyo, Japan (hirotada@nii.ac.jp, keiji@nii.ac.jp). The work of these authors was supported by the Strategic Information and Communications R&D Promotion Programme 031303020 of the Ministry of Internal Affairs and Communications of Japan.

§School of Physics, The University of Melbourne, Victoria, Australia (bentoner@bentoner.com). This work was partly done while this author was at Caltech, Pasadena, and at CWI, Amsterdam. This author's work was supported by the National Science Foundation under grants PHY-0456720 and CCF-0524828, by EU project QAP, by NWO VICI project 639-023-302, and by the Dutch BSIK/BRICKS project.

¶Computer Science Division, University of California, Berkeley, Berkeley, CA 94720 (vidick@eecs.berkeley.edu). This work was partly done while this author was at LRI, Univ. de Paris-Sud, Orsay, and at DI, École Normale Supérieure, Paris, France. This author's work was supported by ARO grant W911NF-09-1-0440 and NSF grant CCF-0905626.

value of such a game, where the input is an explicit description of the game, i.e., a set of possible questions, possible answers, a distribution on questions, and an acceptance predicate for the verifier. A lot of research effort went into determining how hard it is to *approximate* the value of such games, culminating in the celebrated PCP theorem [5, 6], which shows that the value of a two-prover one-round game with a constant number of possible answers is NP-hard to approximate to within some constant. This result has had wide-ranging applications, most notably in the field of hardness of approximation, where it is the basis of many optimal results.

When considering multiprover games in the quantum world, the laws of quantum mechanics allow for a fascinating new effect: the provers can share an arbitrary *entangled* state, on which they may perform any local measurements they like to help them answer the verifier's questions. The fact that entanglement can cause nonclassical correlations is a familiar idea in quantum physics, introduced in a seminal 1964 paper by Bell [7]. Most importantly, there is no physical way to prevent provers from sharing entanglement or to limit how much they have. Compare this to the restriction that the provers cannot communicate during the game, which can be enforced physically by separating the provers in space so that there is no time for a message to travel from one to the other. It is thus a natural and important question to ask how shared entanglement between the provers influences the value of the game, as entanglement can allow for new strategies of the provers. Notice that entanglement can potentially make it either easier or harder to approximate the value of a game, and it is a wide open question as to which of these two effects actually takes place. For example, no algorithm—of any complexity at all—is known to approximate the value of an arbitrary entangled-prover game. One of the most important questions in this field, which we answer in this paper, has been to determine whether computing the value of entangled-prover games is at least NP-hard.

Two recent results give evidence that entangled-prover games might actually be computationally much *easier* than their classical counterparts. First, Cleve et al. [11] showed that in the case of a particular class of two-prover one-round games, XOR games, the value when provers are entangled can be computed (to exponential precision) in polynomial time. In contrast, Håstad [18] showed that for these games *without* entanglement it is NP-hard to approximate the value to within some constant. To prove their result, Cleve et al. [11] show that the maximization problem of the two provers can be written as a semidefinite program (SDP) of polynomial size. It is well known that there are polynomial time algorithms to find the optimum of such SDPs to within exponential precision, and hence there is a polynomial time algorithm to compute the value of these games (to within exponential precision). More precisely, they show that there is an SDP relaxation for the value of the game with the property that its solution can be translated back into a protocol of the provers. This is possible using an inner-product preserving embedding of vectors into two-outcome observables due to Tsirelson [43], which works in the particular case of XOR games. It has been a major open question as to whether this result generalizes beyond XOR games.

In a second recent result giving evidence that entangled-prover games are easy, Kempe, Regev, and Toner [26] showed that even for the class of *unique* games (which contains the class of XOR games), an SDP relaxation of the game gives a good approximation to its value. Hence, for unique games there is a polynomial time algorithm to *approximate* the value of the game to within a constant.

An SDP relaxation is not specific to XOR games or unique games and can be

written for all entangled two-prover games.[1] If the SDP is tight (as in the case of XOR games) or close to tight (as in the case of unique games), there is a polynomial time algorithm to compute or approximate the value of the game. It was speculated that perhaps SDPs can compute, or at least approximate well, the values of more general entangled games. Indeed, the semidefinite programming approach has often been successful when quantum communication is involved: for example, Kitaev and Watrous [28] have shown that SDPs can exactly compute the value of *single-prover* quantum games, Gutoski and Watrous [16] proved that the value of quantum refereed games is as easy to compute as the value of classical refereed games, again via semidefinite programming, and Kitaev [29] showed that the cheating probability for quantum coin-flipping protocols can be computed by SDPs. Moreover, Navascués, Pironio, and Acín [36] recently gave a hierarchy of SDP relaxations to approximate the value of an entangled two-prover game; yet no bounds on the quality of approximation have been proved and these SDPs are in general not of polynomial size.

The major open question is thus to determine if it is easy or hard to compute or even to approximate the value of general entangled-prover games. In particular, would it be possible that the value of such games could be computed or approximated by an SDP?

1.1. Our results. In this paper we resolve the open question above by showing for the first time that it is NP-hard to compute the value of entangled multiprover games in the quantum world. We need to distinguish between two types of entangled games: On one hand, one can still restrict the (possibly entangled) provers to classical communication; we call such games *classical entangled games*. On the other hand, one can also allow the provers to communicate *quantum* messages with a *quantum verifier*; we call these games *quantum entangled games*. In both cases the hardness of computing the value of the game with entangled provers was previously not known,[2] and we show NP-hardness in two cases: for two-prover one-round *quantum entangled games* (in the first part of the paper) and for three-prover one-round *classical entangled games* (in the second part). Then we proceed to show that even *approximating* the value of these two types of games is NP-hard, thus giving the first hardness of approximation results.[3] Our main result can be stated as follows.

THEOREM 1. *There exists a polynomial p such that it is* NP*-hard to decide, for an explicitly given*

1. *two-prover one-round quantum entangled game G or*
2. *three-prover one-round classical entangled game G,*

whether its value is 1 *or at most* $1 - 1/p(|G|)$.[4]

This theorem implies that no polynomial time algorithm can compute the value of an entangled game to within polynomial precision. Given the importance of SDPs in results on entangled games, the following immediate corollary is of interest.

COROLLARY 2. *The success probability of classical entangled three-prover or quantum entangled two-prover games cannot be computed by SDPs of polynomial size, unless* P = NP.

[1] In particular it will also be a relaxation for the value of the classical game (which is not tight in this case, unless P = NP).

[2] A result by Kobayashi and Matsumoto [31] implies that entanglement cannot make it harder to approximate the value of a game unless the number of prior-entangled qubits is superpolynomial.

[3] Obviously the hardness of computation result is implied by the hardness of approximation result. We include it nonetheless in section 3.1 for quantum entangled games to illustrate the main ideas.

[4] See section 2 for a precise definition of the size $|G|$ of G.

The results above leave open the case of *two-prover* one-round *classical* entangled games. Our third result deals with this case, but it has a slightly different flavor: we scale up to games with an exponential number of questions and answers, but which are given succinctly (i.e., the game is given by a description of the circuit of the verifier of size polynomial in $\log |Q|$, the length of the questions). For these games we show that approximating the value to within an inverse polynomial (in $\log |Q|$) is at least as hard as approximating to within a constant the value of classical *single-prover multiround* games with polynomial rounds. Note that this is a better approximation than in the first two results of our paper (where the approximation was to within an inverse polynomial in $|Q|$), but our hardness assumption in this case is weaker than in the previous two results. In particular, combining this with the IP = PSPACE result [35, 39], even with public-coin protocols [15, 40], our result implies PSPACE $\subseteq \mathrm{MIP}^*(2,1)_{1,1-\mathrm{poly}^{-1}}$.[5] Again, no such result was previously known for these games.

All three results turn out to have something in common—in the analysis of all three of them we show that by enforcing certain tests we obtain sets of projectors (which characterize the strategy of the provers) which pairwise "*almost commute*." From this condition we derive a classical strategy for the original classical game in a similar fashion in all three cases.

1.2. Proof ideas and new techniques.

Reduction. We prove our NP-hardness results by a reduction from the hardness of approximation result for classical (nonentangled) games, as implied by the PCP theorem, which we state in the language of games.

THEOREM (PCP theorem [5, 6]). *There is a constant $s < 1$ such that it is* NP*-hard to decide, given a two-prover one-round game with a constant number of answers, whether its value is* 1 *or at most s.*

We start with an instance of such a classical two-prover one-round game and modify it to a two-prover one-round quantum entangled game (or a three-prover one-round classical entangled game in the second part of this paper) with the property that the value of the new entangled game is at least as big as the value of the original game. In other words, if the value of the original game is 1, the value of the new game is still 1. To show that it is NP-hard to *compute* the value of the entangled game we need to show that if the value of the original game is at most s, then the value of the new entangled game is *smaller* than 1. In particular, it suffices to show that if the value of the new entangled game is 1, then the value of the original game is also 1. To show this, we use a successful strategy of the entangled provers to construct a strategy in the original game that achieves a large value (see *Rounding* below).

Because we need only show this when the new value is *exactly* 1, our task is fairly easy once we have established how to modify the game. It requires substantially more work to prove the hardness of approximation result. We perform the same reduction as in the exact case, but now we need to show that if the value of the original game is at most s, then the value of the new entangled game is bounded away from 1 by an inverse polynomial. Equivalently, we have to show that if the value of the new entangled game is above $1 - \varepsilon$ for some inverse-polynomially small ε, then the value of the original classical game is *larger* than s.

[5] This result has recently been improved to hold even for exponentially small soundness by Ito, Kobayashi, and Matsumoto [21].

Modify the game to "immunize" against entanglement. An essential novel technique in our paper is the design of the new games used in our reduction. We design the new games in a way that limits the cheating power of entangled provers. To this end—and this is a crucial difference from previous attempts to upper bound the value of entangled games—we add an extra test to the game. This new test, which can be added generically to *any* two-prover one-round game, significantly limits the use of entanglement by the provers beyond its utility as shared randomness. We hope that this technique of "immunizing" a game against entanglement can be extracted to serve a wider purpose in other contexts where we want to limit the power of entanglement, possibly with cryptographic applications.

In hindsight the fact that we need to modify the games comes as no surprise. Several classical games have been analyzed in the past to show that without modification of the game, entanglement drastically increases their value. One striking example is given by the Magic Square game [4]: Two classical provers can win this game with probability at most 17/18. However, when given entanglement, the provers can win *perfectly*; i.e., they have a strategy that wins with probability 1.

The difficulty in designing the new test lies in making it prevent the provers from using entanglement to coordinate their replies and hence increase their success probability. In the case of quantum games (in the first part of this paper) our idea is to astutely use *quantum* messages and *quantum* tests, and in particular a version of the Swap Test, to enforce (approximately) that the provers do not entangle the message register with the entangled state they share. This allows us to get conditions that involve the provers' operators (describing their strategies) on two different questions. The Swap Test crucially requires that the messages be quantum.

When we analyze classical entangled games (in the second part of our paper) we design a different test: we modify the game by introducing a *third* prover. We use the extra prover to introduce a consistency test that forces two of the provers to give the *same* answer. As a result, to pass this test, the two original provers can use only an entangled state of a specific form; it must be (approximately) *extendable*; i.e., it must be the density matrix of a symmetric tripartite state. There are prior results pointing to the potential usefulness of a third prover to limit the cheating power of entanglement. For example, two entangled provers can cheat in the Odd Cycle game of [11], but if we add a third prover, then entangled provers can perform no better than classical ones [42]. Moreover, after the completion of this work we have learned from Yao [48] about a way to add a third prover to the Magic Square game such that as a result the winning probability of entangled provers is nearly 0.94. See *Related work* below for further discussion of a recent extension of this result.

For our third result on two-prover classical entangled games, our reduction has the same spirit as and analysis similar to the previous two cases: here we start with a *single-prover* multiround game and modify it to a one-round game by introducing a second prover to prevent the first prover from entangling the answers of subsequent rounds. Our modification here mimics a construction of [9] used to prove that PSPACE has (nonentangled) two-prover one-round proof systems.[6]

Rounding. The extra quantum test (resp., the extra prover) allows us to extract a mathematical condition on the operations of the entangled provers. More precisely it turns out that the projectors corresponding to the various questions of the verifier

[6]In fact, we show that the construction in [9] still remains sound even with entangled provers, albeit with a weaker soundness than in the classical case.

pairwise "almost commute" in some sense or "almost do not disturb" the entangled state. This means that the provers' actions are "almost classical," in the sense that they allow us to take any strategy for the entangled game and convert it back to a strategy in the original classical game. We call this conversion *rounding* from a quantum solution to a classical solution, in analogy to the rounding schemes used to convert a solution to an SDP relaxation to a solution of the game. To explain the idea of our new rounding scheme, consider the case of two-prover one-round quantum entangled games. Assume that the provers, when receiving a question from the verifier, perform a projective measurement on their share of the entangled state depending on the question and answer with the outcome they get (it will turn out that this is essentially what the provers can do, even when the game involves quantum communication). In the *exact* case, when the value of the quantum entangled game is 1, the measurements corresponding to different questions *commute* exactly. Hence, there is a common basis in which the projectors corresponding to different answers are all diagonal for all questions. In other words, for each question, the projectors simply define a partition of the basis vectors. The probability that the provers give a certain pair of answers corresponds just to the size of the overlap of the supports of the two corresponding projectors, i.e., to the number of basis vectors that are contained in both of them. We can now construct a classical strategy for the original game, where the provers use shared randomness to sample a basis vector, check which projector/partition contains it, and output the corresponding answer. This classical strategy achieves exactly the same probability distribution of the answers and hence the same value of the game.

Matters become more complicated in the case where the value of the entangled game is larger than $1-\varepsilon$. Now, the provers' measurements corresponding to different questions "almost commute." To exploit this property in a rounding scheme, imagine the following preprocessing step to eliminate entanglement from the strategy: Before the game starts, the provers apply in sequence all possible measurements, corresponding to all possible questions, on a share of the entangled state and write down a list of all the answers they obtain. Then, during the game, when they receive a question from the verifier, they respond with the corresponding answer on their list.[7] Because the measurements almost commute, the answer to any one particular question in this sequential measurement scheme is similarly distributed to the scenario in the entangled game, where the prover performs only the measurement corresponding to that question. This can be seen by "commuting" the corresponding projectors through the list of projectors in the measurement, where each time we commute two operators we lose some small amount of precision. As a result, the success probability of this new unentangled strategy is similar to the one in the entangled game, or at least not too low.

1.3. A new mathematical challenge. As mentioned above, our tests enforce an almost-commuting condition on the operators of the provers. If they commuted exactly, they would be diagonal in a common basis, meaning that the strategy is essentially classical and does not use entanglement. If one could conclude that the operators are *nearly diagonal* in some basis, one could again extract a classical strategy as in the exact case. Hence we reduce proving *constant* hardness of approximation to the question of whether one can approximate our operators by commuting ones.

[7] Obviously, the provers do not really need any entanglement to do this: all they have to do is sample from the joint distribution that corresponds to the distribution of all the answers in this sequence of measurements.

This touches upon a deep question in operator algebra: *Do almost-commuting matrices nearly commute?* Here *almost commuting* means that the commutator is small in some norm, and nearly commuting means that the matrices can be approximated by matrices that are diagonal in a common basis. This famous question was asked for *two Hermitian* matrices by Halmos back in 1976 [17].[8] It was shown subsequently [45],[9] using methods from algebraic topology, that this conjecture is false for two *unitary* matrices. Then, Halmos' conjecture was disproved for the case of three Hermitian matrices [44]. Finally Halmos' conjecture was proved [34] by a "long tortuous argument" [13] using von Neumann algebras, almost 20 years after the conjecture had been publicized. In our case we reduce proving hardness of approximation of the value of an entangled game to the conjecture for a set of pairwise almost-commuting *projectors* (a projector is a Hermitian matrix P such that $P^2 = P$), where the norm is the Frobenius norm $\|A\|_{\mathrm{F}}^2 = \mathrm{Tr}(A^\dagger A)$ (see subsection 3.1).

CONJECTURE. *Let $W_1, \ldots, W_n$ be d-dimensional projectors such that, for some $\varepsilon \geq 0$ and for all $i, j \in \{1, \ldots, n\}$, $\frac{1}{d}\|W_i W_j - W_j W_i\|_{\mathrm{F}}^2 \leq \varepsilon$. Then there exist a $\delta \geq 0$ and pairwise commuting projectors $\tilde{W}_1, \ldots, \tilde{W}_n$ such that $\frac{1}{d}\|W_i - \tilde{W}_i\|_{\mathrm{F}}^2 \leq \delta$ for all $i \in \{1, \ldots, n\}$.*

Our proof for the case of three-prover entangled games[10] shows that the conjecture with a constant δ implies hardness of approximation of the value of entangled games to within a *constant*, i.e., the best possible result. Moreover, when scaled up to the setting of interactive proofs, the conjecture with a constant δ implies inclusion of NEXP in $\mathrm{MIP}^*(3, 1)$ with completeness 1 and soundness bounded away from 1.

For two, three, or a constant number of projectors the conjecture is easy to prove for a constant δ. We do not know if it is true in general.

1.4. Related work. A subset of the authors has obtained weaker results on hardness of approximation of the value of two-prover *quantum* entangled games [27]; the present paper includes and supersedes these results. The techniques developed in this paper have already been applied by Ito et al. [22] to show similar results for *binary* three-prover one-round classical entangled games. They also give a new upper bound for the value of these games; or, as often called in this context, they give a family of new n-partite Tsirelson inequalities. More recently, Ito, Kobayashi, and Matsumoto [21] extended our proof technique and showed how a certain form of oracularization could be used to prove the hardness for *two-prover* one-round classical entangled games, with constant answer size. In the same paper, the authors show that our third result (Theorem 23) holds even if the provers are allowed to use arbitrary *nonsignaling* strategies, and with exponentially small (instead of polynomially close to 1) soundness, in particular giving inclusion of PSPACE in $\mathrm{MIP}^*(2, 1)$. Ito [20] later showed a corresponding upper bound of PSPACE for nonsignaling provers. Combining these two results on nonsignaling provers implies that the class of problems having one-round classical interactive proofs with two nonsignaling provers is equal to PSPACE.

After the completion of this work, Cleve, Gavinsky, and Jain [10] used a connection to private information retrieval schemes to show that succinctly given binary entangled classical games cannot be approximated in polynomial time. Their result does not apply to explicitly given games, as it is based on an exponential expansion

[8] It was asked for the operator norm.

[9] For a simpler, elegant proof see [14].

[10] In the case of two provers, we obtain the weaker condition that *almost all* projectors *almost commute*, which is enough for our proof technique to go through, but it would not allow us to use the conjecture even if it were true.

of the message length.

Finally, we note that the case of single-prover quantum games was recently settled by Jain et al. [23], who showed that QIP = PSPACE.

1.5. Structure. The structure of this paper is as follows: In section 2 we introduce the necessary definitions and notations we use. In section 3 we prove our results on the NP-hardness of quantum entangled two-prover games. To flesh out the ideas, we first prove hardness of *computing* the value of such games, before showing hardness of approximation. In section 4 we show NP-hardness of approximation for three-prover classical entangled games, and in section 5 we give our hardness results for two-prover classical entangled games. We discuss our results and open questions in section 6.

2. Preliminaries. We assume basic knowledge of quantum computation [37, 30].

Games. In this paper we study multiprover games, or cooperative games with imperfect information (henceforth *games*). We will deal only with one-round games played by N cooperative provers against a verifier.

Let Q and A be finite sets and let N be a positive integer. We distinguish three types of games.

Classical game. A classical game is given by a distribution $\pi\colon Q^N \to [0,1]$ and a function $V\colon A^N \times Q^N \to \{0,1\}$.[11] The verifier samples questions $(q_1,\dots,q_N)$ according to π, and sends q_i to prover i, from whom he then receives an answer a_i. He accepts those answers iff $V(a_1,\dots,a_N \mid q_1,\dots,q_N) = 1$. The value of the game is

$$\omega(G) = \max\Bigg[\sum_{\substack{(q_1,\dots,q_N)\in Q^N \\ (a_1,\dots,a_N)\in A^N}} \pi(q_1,\dots,q_N)\Pr(a_1,\dots,a_N \mid q_1,\dots,q_N) \times V(a_1,\dots,a_N \mid q_1,\dots,q_N)\Bigg],$$

where the maximum is taken over all the provers' strategies W_i for $i \in \{1,\dots,N\}$, i.e., functions $W_i\colon Q \times R \to A$ for some domain R ("shared randomness"), and

$$\Pr(a_1,\dots,a_N \mid q_1,\dots,q_N) = \Pr_{r\in R}\Big(W_1(q_1,r) = a_1,\dots,W_N(q_N,r) = a_N\Big).$$

In fact we can assume the strategies to be *deterministic*: there is always some $r \in R$ that maximizes the winning probability, and we can fix it in advance.

Classical entangled game. A classical entangled game is similar to a classical game, except that the provers are now allowed to share an arbitrary state $|\Psi\rangle$ of arbitrary dimension. This increases the set of possible strategies to quantum operations performed on the prover's share of the entangled state. Note that no restrictions on $|\Psi\rangle$ (such as $|\Psi\rangle$ consisting of EPR pairs, or $|\Psi\rangle$ having bounded dimension) are currently known to hold without loss of generality.[12] By standard purification techniques (see, e.g., [11]) one can assume that for each question q each prover performs a projective measurement $\mathcal{W}_q = \{W_q^a\}_{a\in A}$ with outcomes in A (i.e., $\sum_{a\in A} W_q^a = \mathrm{Id}$

[11] We write $V(\cdot,\cdot)$ as $V(\cdot \mid \cdot)$ to clarify the role of the inputs.

[12] In fact, there are games known in which the maximum success probability of the provers goes to 1 with the dimension of their entangled state [33]. Note, however, that these games involve quantum messages and are thus quantum entangled games in our terminology.

and $(W_q^a)^\dagger = W_q^a = (W_q^a)^2$). We will use a superscript "$*$" to indicate entangled-prover games. The value $\omega^*(G)$ of such a game is given by[13]

$$\omega^*(G) = \sup\Big[\sum_{\substack{(q_1,\ldots,q_N)\in Q^N \\ (a_1,\ldots,a_N)\in A^N}} \pi(q_1,\ldots,q_N)\Pr(a_1,\ldots,a_N \mid q_1,\ldots,q_N) \times V(a_1,\ldots,a_N \mid q_1,\ldots,q_N)\Big],$$

where the supremum is taken over all a priori shared states $|\Psi\rangle$ and all projective measurements $(\mathcal{W}_i)_q = \{(W_i)_q^a\}_{a\in A}$ for $i \in \{1,\ldots,N\}$ and $q \in Q$, and the probability now is

$$\Pr(a_1,\ldots,a_N \mid q_1,\ldots,q_N) = \langle\Psi|(W_1)_{q_1}^{a_1} \otimes \cdots \otimes (W_N)_{q_N}^{a_N}|\Psi\rangle.$$

Quantum entangled game. A quantum entangled game is a game in which both the verifier and the provers are quantum, and they exchange quantum messages. We usually denote such a game by G_{q}. The verifier holds N message registers of size $\mathrm{poly}(\log|Q|)$ each, in addition to a private register of size $\mathrm{poly}(\log|Q|)$, all initialized to the state $|0\cdots0\rangle$. He applies a unitary V_1 to all the registers and then sends the message registers to the corresponding provers. By purification we can assume that the kth prover performs a unitary transformation U_k on his message register and his part of the entangled state $|\Psi\rangle$ and then sends the message register back to the verifier. The verifier performs a quantum operation V_2 on the message registers and his private space, followed by a measurement $\{\Pi_{\mathrm{acc}}, \Pi_{\mathrm{rej}}\}$ of his first qubit. The value of a quantum entangled game, ω_{q}^*, is given by

$$\omega_{\mathrm{q}}^*(G_{\mathrm{q}}) = \sup_{|\Psi\rangle, U_1,\ldots,U_N} \mathrm{Tr}(\Pi_{\mathrm{acc}} V_2 U V_1 |\Psi\rangle\langle\Psi| \otimes |0\cdots0\rangle\langle0\cdots0| V_1^\dagger U^\dagger V_2^\dagger),$$

where $U = U_1 \otimes \cdots \otimes U_N$.

Input size. Our complexity parameter is the size of the question set Q. All the other components of the game's distribution (the distribution π, the answer size, the verifier's circuits V_1 and V_2 in the quantum case) are of size polynomial in $|Q|$.[14]

Symmetric games. For convenience we will work with symmetric distributions π and with games with a symmetric verifier and a symmetric optimal strategy. The next lemma shows why this poses no restriction (we need only the case of two provers).

LEMMA 3. *For every classical two-prover game $G = (\pi, V)$ there is a two-prover game $G' = (\pi', V')$ of the same value and twice as many questions such that π' and V' are symmetric under permutation of variables. Moreover, there is an optimal symmetric strategy for G'.*

Proof. The verifier V' in game G' samples q, q' from π. He adds an extra bit register to the questions, and with probability $1/2$ he sends $(q,1)$ to prover 1 and $(q',2)$ to prover 2; otherwise he swaps the two questions. In the second case he swaps the received answers, and in both cases applies the predicate V. For the lower bound observe that if S_1, S_2 is a strategy for G, then the strategy for G' where each prover

[13] We use a supremum because the optimal strategies might not be finite in the case of entangled provers.

[14] In fact all games we consider also have circuits of size $\mathrm{poly}(\log|Q|)$ to prepare the questions and check the answers.

applies S_i if his second message bit is i fares as well as S_1, S_2 (and is symmetric). For the upper bound note that from any strategy S_A, S_B for G' we can construct a strategy for G that fares at least as well by choosing the better of either $S_A(\cdot, 1), S_B(\cdot, 2)$ or $S_B(\cdot, 1), S_A(\cdot, 2)$. Moreover, V' is obviously symmetric under permutation of question-answer pairs. □

In the case where the provers are allowed to share entanglement, we can assume that if π and V have some symmetry, it is mirrored in the optimal prover's strategies.

LEMMA 4. *Let G be an N-prover (classical or quantum) entangled game such that in the classical case $\pi(i_1, \ldots, i_N)$ is symmetric in $i_1, \ldots, i_k$ and in the quantum case the state $V_1|0 \cdots 0\rangle$ is symmetric under simultaneous permutation of the question registers $1, \ldots, k$. Then, given any strategy $P_1, \ldots, P_N$ with entangled state $|\Psi\rangle$ that wins with probability p, there exists a strategy $P'_1, \ldots, P'_N$ with entangled state $|\Psi'\rangle$ and winning probability p such that $P'_1 = \cdots = P'_k$ and $|\Psi'\rangle$ is symmetric with respect to the provers $1, \ldots, k$.*

Proof. Let $\mathfrak{S}_k$ be the set of permutations of $\{1, \ldots, k\}$ and assume, by appropriately padding with extra qubits, that the first k registers of $|\Psi\rangle$ have the same dimension. Define strategies $P'_1, \ldots, P'_N$ as follows: the provers share the entangled state $|\Psi'\rangle = \sum_{\sigma \in \mathfrak{S}_k} |\sigma(1)\rangle \otimes \cdots \otimes |\sigma(k)\rangle \otimes |\Psi^\sigma\rangle$, where the register containing $|\sigma(i)\rangle$ is given to prover i and $|\Psi^\sigma\rangle$ is obtained from $|\Psi\rangle$ by permuting the first k registers according to σ. For $i \leq k$, prover i measures the register containing $|\sigma(i)\rangle$ and behaves as in the strategy $P_{\sigma(i)}$. For $i > k$, $P'_i = P_i$. By symmetry of π and V this new strategy achieves the same winning probability p, and $|\Psi'\rangle$ has the required symmetry properties. □

3. Hardness of two-prover quantum entangled games. In this section we prove Theorem 1 for the case of two-prover quantum entangled games. To better quantify the dependence on the input size, we restate it as a separate result.

THEOREM 5. *There is a constant $s_1 > 0$ such that it is* NP*-hard to decide, given a two-prover quantum entangled game, whether its value is* 1 *or at most* $1 - \varepsilon$ *for* $\varepsilon = \frac{s_1}{|Q|^4}$.

As mentioned in the introduction, we will prove this by a reduction from the PCP theorem. However, to more clearly and cleanly expose the ideas in this proof, we will first prove the simpler statement about NP-hardness of *computing* the value.

3.1. Hardness of computing the value of quantum entangled games.

THEOREM 6. *It is* NP*-hard to decide, given a two-prover quantum entangled game, whether its value is* 1.

We first describe how to modify a two-prover classical game $G_{\mathrm{c}} = (\pi, V)$ with question set Q and answer set A to a two-prover *quantum entangled* game of equal or higher value. We assume that the distribution $\pi(q, q')$ is symmetric (as per Lemma 3, at the expense of doubling the number of questions) and also that there is a nonzero probability for each question to be asked (otherwise we remove it from Q without affecting the value of the game).

The modified quantum game. In the constructed quantum game G_{q} the verifier performs one of the two tests detailed below, each of them with equal probability. In each of those tests, he picks two questions q and q' according to some probability distribution and sends the quantum register $|q, 0\rangle_{\mathrm{A}}$ (resp., $|q', 0\rangle_{\mathrm{B}}$) to the first prover, Alice (resp., to the second prover, Bob). We call the first part of this register the *question register* and the second part the *answer register*. The answer register is initially in some designated state $|0\rangle$, and the provers are expected to write the answer

$a \in A$ to the question $q \in Q$ into this register and then send both registers back. Note that it is important that the prover does not know which test the verifier has chosen to perform.

Classical Test. The verifier samples (q, q') according to the distribution $\pi(q, q')$ and sends $|q, 0\rangle$ to Alice and $|q', 0\rangle$ to Bob. Upon receiving these registers from the provers, he measures them and accepts if the results of the measurement of the question registers are q, q' and the results of the measurement of the answer registers a, a' would win the classical game G_{c}.

Quantum Test. The verifier samples (q, q') according to the distribution $\pi(q)\pi(q')$, where $\pi(q)$ is the marginal of $\pi(q, q')$ and prepares the state

$$\frac{1}{\sqrt{2}}\left(|0\rangle|q, 0\rangle_{\mathrm{A}}|q', 0\rangle_{\mathrm{B}} + |1\rangle|q', 0\rangle_{\mathrm{A}}|q, 0\rangle_{\mathrm{B}}\right).$$

He keeps the first qubit and sends question and answer registers to Alice and Bob. Upon receiving these registers from the provers, he performs a controlled swap on registers A and B controlled by the first qubit (he swaps both the question and the answer registers when the first qubit is $|1\rangle$, and does nothing otherwise). Then he measures his qubit in the basis $\{|+\rangle, |-\rangle\}$[15] and the question registers in the standard basis. He accepts iff the results of the measurement of the question registers are q, q' and the outcome of the measurement of the first qubit is "+."

Note that the value $\omega_{\mathrm{q}}^*(G_{\mathrm{q}})$ of the constructed game G_{q} is obviously at least the value of G_{c}: If the entangled quantum provers, controlled on the question, simply write the answer that the classical unentangled provers would have given to the answer register, they always pass the quantum test, and hence $\omega_{\mathrm{q}}^*(G_{\mathrm{q}}) \geq \omega(G_{\mathrm{c}})/2 + 1/2 \geq \omega(G_{\mathrm{c}})$.

Moreover, the description of the quantum game has essentially the same size as the description of the classical game; i.e., the complexity parameter is the same in both cases. The dimensions of the question and answer registers are $|Q|$ and $|A|$, and the Swap Test requires only extra space that is no more than linear in the number of qubits swapped.

Note that it is only the Swap Test that is genuinely quantum, and it allows us to show that the provers cannot entangle the questions they receive with the entangled state they share too much by relating their actions on two different messages. This test has been used in various settings in the past. In its most simple form it was used in [8] to give a protocol for quantum fingerprinting. However, the test that we perform here is a little more sophisticated, since it implements only a *partial* swap on the two message registers, which might be entangled with the provers' private spaces, on which the verifier is unable to perform the swapping.[16]

A last remark concerns the two different probability distributions used in the two tests. We really need to change the distribution in the quantum test, because it gives us a commutation condition for *all* operators of the provers, corresponding to all different questions. Otherwise, we would obtain it only for pairs of questions q, q' corresponding to a nonzero $\pi(q, q')$, which is not sufficient to round to a classical strategy.

[15] Or, equivalently, he performs a Hadamard transform and measures his qubit in the standard basis.

[16] This partial swap has been used in [28] to show parallelization for single-prover quantum interactive proofs, and in [32] to prove the inclusion QMA(3) $\subseteq$ QMA(2) (conditioned on QMA(2) amplification being possible), where the "2" and "3" refer to the number of Merlins.

Existence of a good classical strategy. We now show that if the value of the quantum game is 1, then there is a strategy for the classical game that wins with probability 1.

LEMMA 7. *If* $\omega_{\mathrm{q}}^*(G_{\mathrm{q}}) = 1$, *then* $\omega(G_{\mathrm{c}}) = 1$.

This implies that if the value of the classical game were less than 1, then the value of the quantum game would be less than 1. Since it is NP-hard to distinguish whether the value of the classical game is 1 or not, it follows that it is NP-hard to decide whether the value of the quantum game is 1.

Proof of Lemma 7. Consider an optimal strategy, which, in particular, passes the quantum test with certainty.[17] Note that if it were not for the controlled swap, the game would be essentially a *classical* entangled game, because question and answer registers are prepared in a classical state and are immediately measured when received by the verifier. We first show that the strategy of the provers is indeed essentially a classical entangled strategy.

CLAIM 8. *There are a shared bipartite state* $|\Psi\rangle_{\mathrm{AB}}$ *and, for each question* $q \in Q$, *a set of projectors* $\{W_q^a\}_{a\in A}$ *acting on each prover's half of* $|\Psi\rangle$ *with* $\sum_{a\in A} W_q^a = \mathrm{Id}$ *such that each prover's transformation can be written as* $|q\rangle|0\rangle|\Psi\rangle \mapsto |q\rangle \sum_a |a\rangle W_q^a|\Psi\rangle$ *and the probability that the verifier measures* a, a' *in the answer registers, given that he sampled* q, q' *in the classical test, is*

$$p_{\mathrm{quant}}(a, a' \mid q, q') = \|W_q^a \otimes W_{q'}^{a'}|\Psi\rangle_{\mathrm{AB}}\|^2.$$

Proof. At the beginning of the protocol the provers share some entangled state $|\Psi'\rangle$ (which includes their private workspace). Alice and Bob apply the same unitary transformation U (recall that we assumed without loss of generality that the strategies in a symmetric quantum game were symmetric). Since the provers pass with probability 1 the classical test, and in particular the check that the question registers are $|q\rangle$ (resp., $|q'\rangle$), it means that they do not change the question registers. Hence it is easy to see that U is block-diagonal and can be written as $U = \sum_q |q\rangle\langle q| \otimes U_q$, where U_q acts on the answer register and half of $|\Psi'\rangle$. Define the operators $\tilde{W}_q^a = (\langle a| \otimes \mathrm{Id}\,) \cdot U_q \cdot (|0\rangle \otimes \mathrm{Id}\,)$, where $|0\rangle$ and $|a\rangle$ act only on the answer register, not on $|\Psi'\rangle$, i.e., $U_q|0\rangle|\Psi'\rangle = \sum_a |a\rangle\tilde{W}_q^a|\Psi'\rangle$. Then it follows that $\sum_a (\tilde{W}_q^a)^\dagger \tilde{W}_q^a = \mathrm{Id}\,$, meaning that the set $\{\tilde{W}_q^a\}_{a\in A}$ defines a superoperator acting on a part of $|\Psi'\rangle$. By standard arguments we can now enlarge the system to a state $|\Psi\rangle$ such that we can replace the $\tilde{W}_q^a$ by projectors W_q^a which give exactly the same outcome probabilities. ∎

We now derive the crucial condition that allows us to define a good classical strategy. It implies that all projectors W_q^a commute with each other (see below in *Rounding*).

CLAIM 9. $W_q^a \otimes W_{q'}^{a'}|\Psi\rangle = W_{q'}^{a'} \otimes W_q^a|\Psi\rangle$ *for all* q, q', a, a'.

Proof. After the controlled swap and the measurement of question registers as q, q', the remaining state of the entire system can be described as

$$\frac{1}{\sqrt{2}} \sum_{a,a'} |a\rangle|a'\rangle\big(|0\rangle(W_q^a \otimes W_{q'}^{a'})|\Psi\rangle + |1\rangle(W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle\big)$$

$$= \frac{1}{2} \sum_{a,a'} |a\rangle|a'\rangle\big(|+\rangle(W_q^a \otimes W_{q'}^{a'} + W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle + |-\rangle(W_q^a \otimes W_{q'}^{a'} - W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle\big),$$

[17] Strictly speaking it could be that such a strategy exists only in the limit of infinite entanglement, so we would have to use a strategy that achieves success probability arbitrarily close to 1. Since in this part we give only the ideas of the rigorous proof in subsection 3.2, we ignore this issue.

and hence the probability of measuring "−" in the extra qubit is $\frac{1}{4}\sum_{a,a'}\|(W_q^a \otimes W_{q'}^{a'} - W_{q'}^{a'} \otimes W_q^a)|\Psi\rangle\|^2$, which must be 0 since the provers pass the quantum test with certainty. □

Rounding. This property of the projectors can be expressed in a different fashion. Assume for simplicity that the shared state is maximally entangled, i.e., $|\Psi\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle_{\mathrm{A}}|i\rangle_{\mathrm{B}}$, and that all projectors are real. Then for any such projectors W, W' we have $\|W \otimes W'|\Psi\rangle\|^2 = \frac{1}{d}\|WW'\|_{\mathrm{F}}^2$, where $\|A\|_{\mathrm{F}}^2 = \mathrm{Tr}(A^\dagger A)$ is the Frobenius norm. The condition in Claim 9 can be rewritten as $\frac{1}{d}\|W_q^a W_{q'}^{a'} - W_{q'}^{a'} W_q^a\|_{\mathrm{F}}^2 = 0$; i.e., the two projectors *commute when acting on the same system.* Hence, in some basis $\{|e_i\rangle\}_{i=1}^d$, all W_q^a are diagonal matrices with only 1 and 0 on the diagonal. In other words, each projector simply defines a *partition* of the basis vectors, and $p(a, a' \mid q, q') = \frac{1}{d}\|W_q^a W_{q'}^{a'}\|_{\mathrm{F}}^2$ measures just the relative *overlap* of the two partitions. With this in mind we can easily design a classical randomized strategy for G_{c} with the same success probability. The provers sample a shared random number $i \in \{1, \ldots, d\}$. When receiving question q they answer with a such that the basis vector $|e_i\rangle$ is in the support of W_q^a. This proof can be generalized to an arbitrary shared state $|\Psi\rangle$ and general projectors; we leave the details to the reader. (In any case Theorem 6 follows from Theorem 5.) □

3.2. Hardness of approximating the value of quantum entangled games. With the intuitions obtained so far we can now tackle the harder case of hardness of approximation. First we give a quick overview. We modify the game in exactly the same way as before. To prove Theorem 5 we now need to show the following lemma for the constant s from the PCP theorem and $\varepsilon = \frac{s_1}{|Q|^4}$ for the constant s_1 in Theorem 5.

LEMMA 10. *If $\omega_{\mathrm{q}}^*(G_{\mathrm{q}}) > 1 - \varepsilon$, then $\omega(G_{\mathrm{c}}) > s$.*

This implies that if the value of the classical game were at most s, then the value of the quantum game would be at most $1 - \varepsilon$. Since, from the PCP theorem, it is NP-hard to distinguish whether the value of the classical game is 1 or at most s, it follows that it is NP-hard to decide whether the value of the entangled quantum game is 1 or at most $1 - \varepsilon$.

To prove Lemma 10, we first show that the strategies of the provers are essentially projective measurements (Claim 11). We then extract the "almost-commuting" conditions on the operators of the provers (Claim 13), which allow us to give a good strategy (described in the introduction) for the original game.

Proof of Lemma 10. Consider a maximizing strategy.[18] It must pass each of the two tests with probability greater than $1 - 2\varepsilon$. Again it is (approximately) true that the strategy of the provers is essentially a *classical* entangled strategy.

CLAIM 11. *There are a shared bipartite state $|\Psi\rangle_{\mathrm{AB}}$ and, for each question $q \in Q$, a set of projectors $\{W_q^a\}_{a\in A}$ acting on each prover's half of $|\Psi\rangle$ with $\sum_{a\in A} W_q^a = \mathrm{Id}$ such that, if we replace each prover's transformation by $|q\rangle|0\rangle|\Psi\rangle \mapsto |q\rangle\sum_a |a\rangle W_q^a|\Psi\rangle$, then the probability of passing each of the tests is greater than $1-6\varepsilon$ and the probability distribution on the answers in the classical test is given by*

$$p_{\mathrm{quant}}(a, a' \mid q, q') = \|W_q^a \otimes W_{q'}^{a'}|\Psi\rangle\|^2.$$

[18] Since it could be that the value of the game is achieved only in the limit of infinite entanglement, we in fact consider a strategy with finite entanglement that has success probability greater than $1 - \varepsilon - \delta$ for some arbitrarily small δ. We will not write this δ in what follows, but the proof goes through for small enough δ, for instance $\delta = O(\varepsilon)$.

Proof. As in the proof of Claim 8 the provers apply the same unitary transformation U, which now is not exactly block-diagonal but in general can be written as $U = \sum_{q,\tilde{q}\in Q} |\tilde{q}\rangle\langle q| \otimes U_{q\tilde{q}}$. Because the verifier in both the classical and the quantum tests measures q, q' in the answer register with probability greater than $1 - 2\varepsilon$, this implies that

$$\mathrm{E}_{(q,q')}\left[\sum_{(\tilde{q},\tilde{q}')\neq(q,q')} \|U_{q\tilde{q}} \otimes U_{q'\tilde{q}'}|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|\Psi'\rangle_{\mathrm{AB}}\|^2\right] < 2\varepsilon,$$

both for when (q, q') is sampled according to $\pi(q, q')$ (from the classical test) and according to $\pi(q)\pi(q')$ (from the quantum test), where we have used symmetry of $|\Psi'\rangle$ for $\|\frac{1}{\sqrt{2}}(|0\rangle U_{q\tilde{q}} \otimes U_{q'\tilde{q}'} + |1\rangle U_{q'\tilde{q}'} \otimes U_{q\tilde{q}})|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|\Psi'\rangle_{\mathrm{AB}}\|^2 = \|U_{q\tilde{q}} \otimes U_{q'\tilde{q}'}|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|\Psi'\rangle_{\mathrm{AB}}\|^2$.

We approximate U by a block-diagonal unitary operator O_U as follows: extend each prover's private space by registers A' and B' of dimension $|Q| + 1$, initialized to $|0\rangle_{\mathrm{A}'}$ and $|0\rangle_{\mathrm{B}'}$, and let $O_U = \sum_q |q\rangle\langle q| \otimes T_q$, where the unitary matrix T_q acts on half of the entangled state and the answer register (together shortened as $|\cdot\rangle$) and A' as

$$T_q|\cdot\rangle|0\rangle_{\mathrm{A}'} = U_{qq}|\cdot\rangle|0\rangle_{\mathrm{A}'} + \sum_{\tilde{q}\neq q} U_{q\tilde{q}}|\cdot\rangle|\tilde{q}\rangle_{\mathrm{A}'}$$

and is extended to a unitary matrix on the other states $|q\rangle_{\mathrm{A}'}$. Observe that

$$\begin{aligned}&\mathrm{E}_{(q,q')}\left[\left\|\left(O_U \otimes O_U - (U \otimes \mathrm{Id}_{\mathrm{A}'}) \otimes (U \otimes \mathrm{Id}_{\mathrm{B}'})\right)|q, 0\rangle_{\mathrm{A}}|q', 0\rangle_{\mathrm{B}}|\Psi'\rangle|0\rangle_{\mathrm{A}'}|0\rangle_{\mathrm{B}'}\right\|^2\right]\\ &\quad = \mathrm{E}_{(q,q')}\left[2\sum_{(\tilde{q},\tilde{q}')\neq(q,q')} \|U_{q\tilde{q}} \otimes U_{q'\tilde{q}'}|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|\Psi'\rangle\|^2\right] < 4\varepsilon,\end{aligned}$$

again both for when (q, q') is sampled according to $\pi(q, q')$ and according to $\pi(q)\pi(q')$. This means that for purposes of analysis we can replace Alice and Bob's transformation U by O_U, thereby replacing the transformation $U \otimes U$ on the message registers and $|\Psi\rangle$ by the transformation $O_U \otimes O_U$ on the message space and $|\tilde{\Psi}\rangle = |\Psi'\rangle|0\rangle_{\mathrm{A}'}|0\rangle_{\mathrm{B}'}$, at the expense of an error 4ε in statistical distance on the answer probabilities of the classical test and the outcome probabilities in the quantum test. Since O_U is block-diagonal, the remainder of this claim follows exactly as in the proof of Claim 8. ∎

The Swap Test now allows us to establish a set of inequalities which capture the "almost-commuting" property of the operators. In what follows we will repeatedly use the following easy-to-verify fact.

FACT 12. *Let $W^1, \ldots, W^k$ be projectors such that $\sum_i W^i = \mathrm{Id}$. Then, for any vector $|\Psi\rangle$, $\sum_i \|W^i|\Psi\rangle\|^2 = \||\Psi\rangle\|^2$.*

CLAIM 13.

$$\sum_{i,j=1}^{|Q|} \pi(q_i)\pi(q_j) \sum_{a_i,a'_j} \|(W_{q_i}^{a_i} \otimes W_{q_j}^{a'_j} - W_{q_j}^{a'_j} \otimes W_{q_i}^{a_i})|\Psi\rangle\|^2 < 24\varepsilon, \tag{1a}$$

$$\sum_{i=1}^{|Q|} \pi(q_i) \sum_{a_i} \|(W_{q_i}^{a_i} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_i}^{a_i})|\Psi\rangle\|^2 < 9 \cdot 24 \cdot \varepsilon. \tag{1b}$$

Proof. As in the proof of Claim 9, the left-hand side of inequality (1a) is four times the probability of measuring the first qubit in "$-$" in the quantum test. For

inequality (1b), using Fact 12, for any fixed q_j the following holds:

$$\begin{aligned}\|(W_{q_i}^{a_i}\otimes \mathrm{Id} - \mathrm{Id}\otimes W_{q_i}^{a_i})|\Psi\rangle\|^2 &= \sum_{a_j',a_j''} \|(W_{q_j}^{a_j'}W_{q_i}^{a_i}\otimes W_{q_j}^{a_j''} - W_{q_j}^{a_j'}\otimes W_{q_j}^{a_j''}W_{q_i}^{a_i})|\Psi\rangle\|^2\\ &\le \sum_{a_j',a_j''}\Big(\|(W_{q_j}^{a_j'}W_{q_i}^{a_i}\otimes W_{q_j}^{a_j''} - W_{q_j}^{a_j'}W_{q_j}^{a_j''}\otimes W_{q_i}^{a_i})|\Psi\rangle\|\\ &\qquad + \|(W_{q_j}^{a_j'}W_{q_j}^{a_j''}\otimes W_{q_i}^{a_i} - W_{q_i}^{a_i}\otimes W_{q_j}^{a_j''}W_{q_j}^{a_j'})|\Psi\rangle\|\\ &\qquad + \|(W_{q_i}^{a_i}\otimes W_{q_j}^{a_j''}W_{q_j}^{a_j'} - W_{q_j}^{a_j'}\otimes W_{q_j}^{a_j''}W_{q_i}^{a_i})|\Psi\rangle\|\Big)^2.\end{aligned}$$

We can bound the square of the sum of the three norms by three times the sum of the norms squared, and summing over a_i, averaging over q_i, q_j, and using $W_q^a W_q^{a'} = \delta_{a,a'}W_q^a$ for the second norm and Fact 12 for the other two, we get three terms that are each bounded using inequality (1a), concluding the proof of inequality (1b). ∎

Rounding to a classical strategy. Order the questions in Q such that $\pi(q_1) \ge \pi(q_2) \ge \cdots \ge \pi(q_n)$. Define a joint distribution on answers $a_1,\dots,a_n$ as

$$D(a_1,\dots,a_n) = \|(W_{q_n}^{a_n}\cdots W_{q_1}^{a_1}\otimes \mathrm{Id})|\Psi\rangle\|^2.$$

Fact 12 shows that D is a probability distribution: $\sum_{a_1,\dots,a_n} D(a_1,\dots,a_n) = 1$.

We can interpret D as follows: Before the game starts, the provers produce a joint list of answers $a_1,\dots,a_n$ as follows. They take the first part of $|\Psi\rangle$ and perform the projective measurement corresponding to question q_1. They obtain an outcome a_1, which they record. They then take the postmeasurement state and perform on it the measurement corresponding to question q_2, and so on, each time using the postmeasurement state of one measurement as the input state of the next measurement. The probability that the provers record answers $a_1,\dots,a_n$ is precisely $D(a_1,\dots,a_n)$.

Obviously neither quantum states nor measurements are needed to implement this constructed classical strategy. Before the game starts, the provers simply compute D for all inputs and sample from D using their shared randomness. When presented with questions q_i, q_j they give the answer a_i, a_j, ignoring all other answers in their sample. Hence the probability of answering a_i, a_j in this case is given by the marginal of D with respect to a_i and a_j, which we denote by $p_{\mathrm{class}}(a_i, a_j \mid q_i, q_j)$.

LEMMA 14. *The (weighted) statistical distance between p_{class} and p_{quant} is*

$$\Delta(p_{\mathrm{class}}, p_{\mathrm{quant}}) = \sum_{q,q'}\pi(q,q')\sum_{a,a'}\big|p_{\mathrm{class}}(a,a' \mid q,q') - p_{\mathrm{quant}}(a,a' \mid q,q')\big| < 70|Q|\varepsilon^{\frac{1}{4}}.$$

Let us first show how this proves Lemma 10. Since the quantum strategy of the provers passes the classical test with probability greater than $1-6\varepsilon$, this means that the resulting classical strategy wins the original game with probability greater than $1-6\varepsilon-\Delta(p_{\mathrm{class}}, p_{\mathrm{quant}})$ (where Δ is the dominating term), which we want to be larger than s. This is achieved for $\varepsilon = \frac{s_1}{|Q|^4}$ for a sufficiently small constant s_1. ∎

Proof of Lemma 14. Let q_i and q_j be two questions. For convenience, let us introduce the notation $\sum_{\boldsymbol{a}}$ to denote summing over $a_1,\dots,a_n$ and $\sum_{\boldsymbol{a}_{\neg i,j}}$ to denote summing over all $a_1,\dots,a_n$ except a_i and a_j. Then the probability of answering (a_i,a_j) to (q_i,q_j) is $p_{\mathrm{class}}(a_i,a_j \mid q_i,q_j) = \sum_{\boldsymbol{a}_{\neg i,j}}\|(W_{q_n}^{a_n}\cdots W_{q_1}^{a_1}\otimes \mathrm{Id})|\Psi\rangle\|^2$ in the

classical strategy and $p_{\text{quant}}(a_i, a_j \mid q_i, q_j) = \|W_{q_i}^{a_i} \otimes W_{q_j}^{a_j} |\Psi\rangle\|^2$ in the quantum strategy. We wish to bound

$$\sum_{a_i,a_j} \left| p_{\text{class}}(a_i, a_j \mid q_i, q_j) - p_{\text{quant}}(a_i, a_j \mid q_i, q_j) \right| = \sum_{a_i,a_j} \left| \sum_{\boldsymbol{a}_{\neg i,j}} \|(W_{q_n}^{a_n} \cdots W_{q_1}^{a_1} \otimes \mathrm{Id}\,)|\Psi\rangle\|^2 - \|W_{q_i}^{a_i} \otimes W_{q_j}^{a_j} |\Psi\rangle\|^2 \right|.$$

We now use a hybrid argument to go from the classical to the quantum probability. The point is to eliminate the excess W_q^a in p_{class} with the help of Fact 12, which results in eliminating a sum over a that involves a W_q^a on the *left* side of all other operators in $\|\cdot\|^2$. To get all unwanted W_q^a to be on the left, we move matrices from one register to the other whenever they are on the *right*, closest to $|\Psi\rangle$, at the expense of some error which we can bound using the inequalities (1a) and (1b). More precisely we use the triangle inequality for matrices X, W, Y, W',

$$\left| \|(XW \otimes YW')|\Psi\rangle\| - \|(XW' \otimes YW)|\Psi\rangle\| \right| \leq \|(X \otimes Y)[W \otimes W' - W' \otimes W]|\Psi\rangle\|, \tag{2}$$

where X and Y will be sequences of W_q^a's and W or W' will be either one of the W_q^a's or the identity.

To describe the sequence along which we move the matrices around, let us use the shorthand notation W_k for $W_{q_k}^{a_k}$. At each step we will interchange either $W_k \otimes \mathrm{Id} \leftrightarrow \mathrm{Id} \otimes W_k$ or $W_i \otimes W_k \leftrightarrow W_k \otimes W_i$ whenever they are on the right. If $i > j$, we proceed according to the sequence

$$\begin{aligned} &W_n \cdots W_1 \otimes \mathrm{Id} \to W_n \cdots W_2 \otimes W_1 \to W_n \cdots W_3 \otimes W_1 W_2 \\ &\quad \to \cdots \to W_n \cdots W_{i+1} W_i \otimes W_1 \cdots W_{i-1} \to W_n \cdots W_{i+1} W_{i-1} \otimes W_1 \cdots W_{i-2} W_i \\ &\quad \to W_n \cdots W_{i+1} W_{i-1} W_i \otimes W_1 \cdots W_{i-2} \to W_n \cdots W_{i+1} W_{i-1} W_{i-2} \otimes W_1 \cdots W_{i-3} W_i \\ &\quad \to \cdots \to W_n \cdots W_{i+1} W_{i-1} \cdots W_{j+1} W_i \otimes W_1 \cdots W_j. \end{aligned}$$

Note that the last term in the sequence, when summed over $\boldsymbol{a}_{\neg i,j}$, cancels the quantum term because of Fact 12, i.e., $\sum_{\boldsymbol{a}_{\neg i,j}} \|W_n \cdots W_{j+1} W_i \otimes W_1 \cdots W_j |\Psi\rangle\|^2 = \|W_i \otimes W_j |\Psi\rangle\|^2 = p_{\text{quant}}(a_i, a_j \mid q_i, q_j)$. Now we can write a telescopic sum according to this sequence as

$$\begin{aligned} &\sum_{a_i,a_j} \left| p_{\text{class}}(a_i, a_j \mid q_i, q_j) - p_{\text{quant}}(a_i, a_j \mid q_i, q_j) \right| \\ &\quad = \sum_{a_i,a_j} \left| \sum_{\boldsymbol{a}_{\neg i,j}} \|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\|^2 - \sum_{\boldsymbol{a}_{\neg i,j}} \|W_n \cdots W_2 \otimes W_1 |\Psi\rangle\|^2 \right. \\ &\qquad \left. + \sum_{\boldsymbol{a}_{\neg i,j}} \|W_n \cdots W_2 \otimes W_1 |\Psi\rangle\|^2 - \sum_{\boldsymbol{a}_{\neg i,j}} \|W_n \cdots W_3 \otimes W_1 W_2 |\Psi\rangle\|^2 + \cdots \right| \\ &\quad \leq \sum_{\boldsymbol{a}} \left| \|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\|^2 - \|W_n \cdots W_2 \otimes W_1 |\Psi\rangle\|^2 \right| + \sum_{\boldsymbol{a}} \left| \cdots \right| + \cdots, \end{aligned}$$

where we used the triangle inequality. Using $|a^2 - b^2| = |a - b| \cdot |a + b|$ and the triangle inequality (2), the first term is bounded by

$$\sum_{\boldsymbol{a}} \big\| W_n \cdots W_2 [W_1 \otimes \mathrm{Id} - \mathrm{Id} \otimes W_1] |\Psi\rangle \big\| \times \big(\|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\| + \|W_n \cdots W_2 \otimes W_1 |\Psi\rangle\| \big)$$
$$\leq \sqrt{\sum_{\boldsymbol{a}} \big\| W_n \cdots W_2 [W_1 \otimes \mathrm{Id} - \mathrm{Id} \otimes W_1] |\Psi\rangle \big\|^2} \times \sqrt{\sum_{\boldsymbol{a}} \big(\|W_n \cdots W_1 \otimes \mathrm{Id}\ |\Psi\rangle\| + \|W_n \cdots W_2 \otimes W_1 |\Psi\rangle\| \big)^2},$$

where we used the Cauchy–Schwarz inequality. We obtain similar expressions for all other terms. We can bound the second square root by $\sqrt{2+2} = 2$ using the inequality $(a+b)^2 \leq 2a^2 + 2b^2$ and Fact 12. Assembling all the terms, and using Fact 12 to eliminate all the matrices to the left of the square brackets, we obtain

$$\begin{aligned} \sum_{a_i, a_j} \big| p_{\mathrm{class}}(a_i, a_j \mid q_i, q_j) - p_{\mathrm{quant}}(a_i, a_j \mid q_i, q_j) \big| \\ \leq 2 \sum_{i'=1}^{i-1} \sqrt{\sum_{a_{i'}} \big\| [W_{i'} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{i'}] |\Psi\rangle \big\|^2} \\ + 2(|i-j|-1) \sqrt{\sum_{a_i} \big\| [\mathrm{Id} \otimes W_i - W_i \otimes \mathrm{Id}\,] |\Psi\rangle \big\|^2} \\ + 2 \sum_{i'=j+1}^{i-1} \sqrt{\sum_{a_i, a_{i'}} \big\| [W_i \otimes W_{i'} - W_{i'} \otimes W_i] |\Psi\rangle \big\|^2}. \end{aligned} \tag{3}$$

For $j > i$ we obtain exactly the same sequence and the same bounds in inequality (3) with i and j interchanged. The only difference is that now the last term in the sequence, when summed over $\boldsymbol{a}_{\neg i,j}$, gives $\|W_j \otimes W_i |\Psi\rangle\|^2$, so we need to use symmetry of $|\Psi\rangle$ to conclude that this equals $\|W_i \otimes W_j |\Psi\rangle\|^2$. For $i = j$ we follow the sequence until $W_n \cdots W_{i+1} W_i \otimes W_1 \cdots W_{i-1}$ and then use $W_i = W_i^2$ to continue as $W_n \cdots W_{i+1} W_i W_i \otimes W_1 \cdots W_{i-1} \to W_n \cdots W_i \otimes W_1 \cdots W_{i-1} W_i$, so we just get the first term of the right-hand side of inequality (3), but it is summed until i.

Now $\Delta(p_{\mathrm{class}}, p_{\mathrm{quant}})$ is bounded by the average over (q_i, q_j) picked according to the distribution π of the sum of the three terms appearing in the right-hand side of inequality (3). We show how to bound each of them. For the first term

$$\begin{aligned} 2 \sum_{i,j=1}^{|Q|} \pi(q_i, q_j) \sum_{i'=1}^{i} \sqrt{\sum_{a_{i'}} \big\| \big(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}} \big) |\Psi\rangle \big\|^2} \\ = 2 \sum_{i=1}^{|Q|} \pi(q_i) \sum_{i'=1}^{i} \sqrt{\sum_{a_{i'}} \big\| \big(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}} \big) |\Psi\rangle \big\|^2} \\ \leq 2 \sum_{i=1}^{|Q|} \sum_{i'=1}^{|Q|} \pi(q_{i'}) \sqrt{\sum_{a_{i'}} \big\| \big(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}} \big) |\Psi\rangle \big\|^2} \\ \leq 2|Q| \sqrt{\sum_{i'=1}^{|Q|} \pi(q_{i'}) \sum_{a_{i'}} \big\| \big(W_{q_{i'}}^{a_{i'}} \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{q_{i'}}^{a_{i'}} \big) |\Psi\rangle \big\|^2} \\ < 2|Q| \sqrt{9 \cdot 24 \varepsilon}, \end{aligned}$$

where the first equality uses the fact that the inner sum does not depend on j, the second inequality uses $\pi(q_i) \leq \pi(q_{i'})$, the third inequality uses the fact that the square of the expectation is not greater than the expectation of the square, and the last inequality uses inequality (1b). The second term can be bounded in a similar fashion:

$$2\sum_{i,j=1}^{|Q|}\pi(q_i,q_j)(|i-j|-1)\sqrt{\sum_{a_i}\left\|\left(\mathrm{Id}\otimes W_{q_i}^{a_i}-W_{q_i}^{a_i}\otimes\mathrm{Id}\right)|\Psi\rangle\right\|^2}$$
$$\leq 2|Q|\sum_{i=1}^{|Q|}\pi(q_i)\sqrt{\sum_{a_i}\left\|\left(\mathrm{Id}\otimes W_{q_i}^{a_i}-W_{q_i}^{a_i}\otimes\mathrm{Id}\right)|\Psi\rangle\right\|^2} < 2|Q|\sqrt{9\cdot 24\varepsilon}.$$

Finally the last term, using again that the inner sum does not depend on j, that the square of the expectation is bounded by the expectation of the square and the Cauchy–Schwarz inequality for the sum over i', can be bounded by

$$2\sum_{i=1}^{|Q|}\pi(q_i)\sum_{i'=1}^{i-1}\sqrt{\sum_{a_i,a_{i'}}\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|^2}$$
$$\leq 2\left(\sum_{i=1}^{|Q|}\pi(q_i)\left(\sum_{i'=1}^{i-1}\sqrt{\sum_{a_i,a_{i'}}\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|^2}\ \right)^2\right)^{1/2} \tag{4}$$
$$\leq 2\sqrt{|Q|}\left(\sum_{i=1}^{|Q|}\pi(q_i)\sum_{i'=1}^{i-1}\sum_{a_i,a_{i'}}\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|^2\right)^{1/2}.$$

We decompose the sum inside the square root in the last line of inequality (4) into two parts with $\pi(q_i) \geq 1/h$ and $\pi(q_i) < 1/h$ (with h to be determined later). If $\pi(q_i) \geq 1/h$, then $\pi(q_{i'}) \geq 1/h$ for $i' \leq i$, so $1 \leq h\pi(q_{i'})$. Therefore, using inequality (1a), the term in parentheses in the last line of inequality (4) is bounded by

$$\sum_{i:\pi(q_i)\geq\frac{1}{h}}\sum_{i'=1}^{i-1}h\pi(q_{i'})\pi(q_i)\sum_{a_i,a_{i'}}\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|^2$$
$$+\frac{1}{h}\sum_{i:\pi(q_i)<\frac{1}{h}}\sum_{i'=1}^{i-1}\sum_{a_i,a_{i'}}\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|^2 < 24h\varepsilon+\frac{4|Q|^2}{h},$$

where we have bounded the first part using inequality (1a) and the second part using the triangle inequality, the symmetry of $|\Psi\rangle$, and Fact 12:

$$\sum_{a_i,a_{i'}}\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}-W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|^2$$
$$\leq\sum_{a_i,a_{i'}}\left(\left\|\left(W_{q_i}^{a_i}\otimes W_{q_{i'}}^{a_{i'}}\right)|\Psi\rangle\right\|+\left\|\left(W_{q_{i'}}^{a_{i'}}\otimes W_{q_i}^{a_i}\right)|\Psi\rangle\right\|\right)^2\leq 4.$$

The optimal h is $|Q|/\sqrt{6\varepsilon}$, which gives a bound of $4\cdot 24^{1/4}|Q|\varepsilon^{1/4}$ for the third (dominant) term in $\Delta(p_{\mathrm{class}}, p_{\mathrm{quant}})$ (after taking the square root). Hence $\Delta(p_{\mathrm{class}}, p_{\mathrm{quant}}) < 70|Q|\varepsilon^{1/4}$. ∎

4. Hardness of three-prover classical entangled games. In this section we prove Theorem 1 for three-prover classical entangled games, which we now state.

THEOREM 15. *There is a constant $s_2 > 0$ such that it is* NP*-hard to decide, given a three-prover classical entangled game with a constant number of answers, whether its value is* 1 *or at most* $1 - \varepsilon$ *for* $\varepsilon = \frac{s_2}{|Q|^2}$.

As in the case of quantum entangled games, we will prove this by a reduction from the PCP theorem. This time, we modify the game to a three-prover classical entangled game, as described in the introduction, which essentially has the same number of answers.

We begin by describing how to modify any two-prover classical game $G = (\pi, V)$ (which is assumed to be symmetric per Lemma 3) to a three-prover classical game G' of equal or higher value.

The modified three-prover game. In the constructed game G' the verifier chooses one of the provers uniformly at random. Rename the chosen prover Alice and call the other provers Bob and Cleve. The verifier samples questions q and q' according to $\pi(q, q')$. He sends question q to both Alice and Cleve and question q' to Bob. He receives answers a, a', and a'', respectively, and accepts iff the following are both true.

Classical Test. The answers of Alice and Bob would win the game G; i.e., the answers a and a' satisfy $V(a, a' \mid q, q') = 1$.

Consistency Test. Alice and Cleve give the same answer, i.e., $a = a''$.

Note that unlike the quantum case, the verifier performs both tests at the same time. The consistency test plays the role of the Swap Test, limiting the advantage gained by sharing entanglement.

Again it is clear that the value of the constructed game is at least as large as the value of the original game G: if the provers reply according to an optimal classical strategy (which can be assumed to be symmetric per Lemma 3), they always pass the consistency test. Also, it is clear in this case that the size of the description of the constructed game is linearly related to the size of the description of the original game; hence we have the same complexity parameter.

To prove Theorem 15, we need to show the following lemma.

LEMMA 16. *If $\omega^*(G') > 1 - \varepsilon$, then $\omega(G) > s$.*

Here $\varepsilon = \frac{s_2}{|Q|^2}$ for the constant s_2 in Theorem 15 and the constant s is from the PCP theorem.

Proof. Consider an entangled strategy for G' that succeeds with probability greater than $1 - \varepsilon$.[19] Since the game G' is symmetric, we can assume that this strategy is symmetric per Lemma 4. Suppose that the provers share a symmetric state $|\Psi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{B} \otimes \mathcal{H}_\mathrm{C}$, where each $\mathcal{H}_\mathrm{A}$, $\mathcal{H}_\mathrm{B}$, and $\mathcal{H}_\mathrm{C}$ is isomorphic to a same $\mathcal{H}$. Let $\rho_\mathrm{AB} = \mathrm{Tr}_{\mathcal{H}_\mathrm{C}} |\Psi\rangle\langle\Psi|$ be the reduced state of $|\Psi\rangle\langle\Psi|$ on Alice and Bob. When asked question q_i, each prover measures his part of $|\Psi\rangle$. Following standard arguments (extending the private space of the provers) we can assume that this measurement is projective. Let $W_{q_i}^{a_i}$ be the projector corresponding to question q_i and answer a_i. This defines the entangled strategy for G'; it passes the classical test with probability

$$\pi_1 = \sum_{a,a',q,q'} \pi(q, q') V(a, a' \mid q, q') p_\mathrm{ent}(a, a' \mid q, q'),$$

[19] Again, as in section 3.2, we in fact consider a strategy with finite entanglement that has success probability greater than $1 - \varepsilon - \delta$ for some $\delta = O(\varepsilon)$, which we will not write.

where

$$p_{\text{ent}}(a, a' \mid q, q') = \operatorname{Tr}\left(W_q^a \otimes W_{q'}^{a'} \rho_{\text{AB}}\right) = \langle \Psi | W_q^a \otimes W_{q'}^{a'} \otimes \text{Id} \, | \Psi \rangle. \tag{5}$$

It passes the consistency test with probability $\pi_2 = \sum_q \pi(q)\pi_2(q)$, where $\pi(q)$ is the marginal of $\pi(q, q')$ and

$$\pi_2(q) = \sum_a \operatorname{Tr}\left(W_q^a \otimes W_q^a \rho_{\text{AB}}\right) = \sum_a \langle \Psi | W_q^a \otimes W_q^a \otimes \text{Id} \, | \Psi \rangle, \tag{6}$$

where we made use of the symmetry. Note that $\pi_1, \pi_2 > 1 - \varepsilon$.

Equations (5) and (6) clarify the role of the third prover, Cleve. The main purpose of introducing the third prover is *not* to allow the two tests to be performed at the same time: Indeed, it is possible to modify the protocol so that the verifier chooses two of the provers at random (say Alice and Bob) and sends questions only to them, not interacting with the third prover at all.[20] The presence of the third prover would not be important if the provers were executing a classical strategy, but it can (and does) make a difference if their strategy requires entanglement. Indeed, if there were only two provers, then they could share any state ρ_{AB}, whereas here we require that ρ_{AB} be *extendable*; i.e., it must be the reduced density matrix of a symmetric tripartite state. To give a concrete example, it is not possible for ρ_{AB} to be the maximally entangled state $|\Psi^-\rangle\langle\Psi^-|$. This is termed *monogamy of entanglement* [46].

Rounding to a classical strategy. We construct a classical strategy for G from the entangled strategy for G' in a fashion similar to the case of quantum entangled games, with

$$D(a_1, \ldots, a_n, a'_1, \ldots, a'_n) = \left\| W_{q_n}^{a_n} \cdots W_{q_1}^{a_1} \otimes W_{q_n}^{a'_n} \cdots W_{q_1}^{a'_1} \otimes \text{Id} \, | \Psi \rangle \right\|^2,$$

where $q_1, \ldots, q_n$ is an ordering of the questions in Q such that $\pi(q_1) \geq \pi(q_2) \geq \cdots \geq \pi(q_n)$.[21] As before, we define $p_{\text{class}}(a_i, a'_j \mid q_i, q_j)$ to be the marginal of D on a_i, a'_j. The structure of our proof that this strategy is a good one is very similar to the quantum case. The details, however, are a little different.

LEMMA 17. *The (weighted) statistical distance between* p_{class} *and* p_{ent} *is*

$$\Delta(p_{\text{class}}, p_{\text{ent}}) = \sum_{q,q'} \pi(q, q') \sum_{a,a'} \left| p_{\text{class}}(a, a' \mid q, q') - p_{\text{ent}}(a, a' \mid q, q') \right| < 12|Q|\sqrt{\varepsilon}.$$

We first show how this lemma proves Lemma 16. Since the strategy in the entangled game passes the classical test with probability greater than $1 - \varepsilon$, the classical strategy succeeds in the original game with probability greater than $1 - \varepsilon - \Delta(p_{\text{class}}, p_{\text{ent}}) > 1 - \varepsilon - 12|Q|\sqrt{\varepsilon}$. For $\varepsilon = \frac{s_2}{|Q|^2}$ and for sufficiently small constant s_2, this probability is larger than s. ∎

Lemma 17 is the corresponding version of Lemma 14. Why is it true? Rather than showing that the order of measurements is not important as we did in the quantum case (although it will turn out in hindsight that this is true), we show that each

[20] With probability p, he sends them different questions and performs the classical test; with probability $1 - p$, he sends the same question and performs the consistency test—this modification does not materially change our conclusions, but it does weaken the bounds in Theorem 15.

[21] Note that D differs slightly from subsection 3.2. Here each prover gets a separate list of answers. This form is more convenient here.

measurement does not disturb ρ_{AB} very much. The key observation is as follows. Assume the provers pass the consistency test with high probability. If a particular measurement result occurs with certainty, the quantum state cannot be changed by the measurement. We use this fact in the following way: suppose Cleve were to perform the measurement corresponding to question q and assume he obtains an outcome a. Then, if Alice is asked question q, she must also give answer a with high probability. Thus her measurement does not change the quantum state much. However, since quantum theory is nonsignaling, it cannot matter who measured first. It follows that Alice's measurement does not change ρ_{AB} much. Note that only the bipartite state ρ_{AB} is approximately unchanged—Alice's measurement can change the tripartite state $|\Psi\rangle\langle\Psi|$ considerably. We then use a hybrid argument to show that performing all the measurements one after the other also leaves ρ_{AB} approximately unchanged. This part of the proof mirrors the proof of Lemma 14.

Proof of Lemma 17. Let $\mathcal{W}_q$ be the superoperator corresponding to the projective measurement performed on question q; i.e., $\mathcal{W}_q(\sigma) = \sum_a W_q^a \sigma (W_q^a)^\dagger$ is the postmeasurement state after performing $\{W_q^a\}$ on state σ.

To quantify how much a measurement changes a state we use Winter's Gentle Measurement Lemma.

LEMMA 18 (Lemma I.4 in [47]). *Let ρ be a state and X be a positive matrix with $X \leq \mathrm{Id}$ and $0 \leq \mathrm{Tr}\rho X$. Then*

$$\left\|\rho - \sqrt{X}\rho\sqrt{X}\right\|_{\mathrm{tr}} \leq 3\sqrt{1 - \mathrm{Tr}X\rho}.$$

The following simple corollary quantifies how much the measurement $\mathcal{W}_q \otimes \mathrm{Id}$ changes ρ_{AB}.

CLAIM 19. *The trace distance between $\mathcal{W}_q \otimes \mathrm{Id}\,(\rho_{\mathrm{AB}})$ and ρ_{AB} is bounded by*

$$\|\mathcal{W}_q \otimes \mathrm{Id}\,(\rho_{\mathrm{AB}}) - \rho_{\mathrm{AB}}\|_{\mathrm{tr}} \leq 6\sqrt{1 - \pi_2(q)}.$$

Proof. Using the relations $\mathcal{W}_q \otimes \mathrm{Id}\,(\rho_{\mathrm{AB}}) = \mathrm{Tr}_{\mathcal{H}_{\mathrm{C}}}(\mathcal{W}_q \otimes \mathrm{Id} \otimes \mathrm{Id}\,(|\Psi\rangle\langle\Psi|))$ and $\rho_{\mathrm{AB}} = \mathrm{Tr}_{\mathcal{H}_{\mathrm{C}}}(\mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|))$,

$$\begin{aligned}
&\|\mathcal{W}_q \otimes \mathrm{Id}\,(\rho_{\mathrm{AB}}) - \rho_{\mathrm{AB}}\|_{\mathrm{tr}} \\
&\quad\leq \|\mathcal{W}_q \otimes \mathrm{Id} \otimes \mathrm{Id}\,(|\Psi\rangle\langle\Psi|) - \mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|)\|_{\mathrm{tr}} \\
&\quad\leq \Big\|\mathcal{W}_q \otimes \mathrm{Id} \otimes \mathrm{Id}\,(|\Psi\rangle\langle\Psi|) - \sum_a W_q^a \otimes \mathrm{Id} \otimes W_q^a |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes W_q^a\Big\|_{\mathrm{tr}} \\
&\qquad + \Big\|\sum_a W_q^a \otimes \mathrm{Id} \otimes W_q^a |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes W_q^a - \mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|)\Big\|_{\mathrm{tr}} \\
&\quad\leq 2\Big\|\sum_a W_q^a \otimes \mathrm{Id} \otimes W_q^a |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes W_q^a - \mathrm{Id} \otimes \mathrm{Id} \otimes \mathcal{W}_q(|\Psi\rangle\langle\Psi|)\Big\|_{\mathrm{tr}} \\
&\quad\leq 6\sqrt{1 - \pi_2(q)}
\end{aligned}$$

by monotonicity of the trace distance under partial trace, the triangle inequality, and symmetry and then taking $\rho = \bigoplus_a W_q^a \otimes \mathrm{Id} \otimes \mathrm{Id}\ |\Psi\rangle\langle\Psi| W_q^a \otimes \mathrm{Id} \otimes \mathrm{Id}$ and $X = \bigoplus_a \mathrm{Id} \otimes \mathrm{Id} \otimes W_q^a$ in Lemma 18. ∎

For $1 \leq i, j \leq n$, let

$$\rho_{\mathrm{AB}}(i,j) = (\mathcal{W}_{q_{i-1}} \circ \cdots \circ \mathcal{W}_{q_1}) \otimes (\mathcal{W}_{q_{j-1}} \circ \cdots \circ \mathcal{W}_{q_1})\rho_{\mathrm{AB}}.$$

Then

$$p_{\mathrm{class}}(a_i, a'_j \mid q_i, q'_j) = \mathrm{Tr}\Big(\big(W_{q_i}^{a_i} \otimes W_{q'_j}^{a'_j}\big)\rho(i,j)\Big).$$

Hence we can bound $\sum_{a_i,a'_j} |p_{\text{class}}(a_i, a'_j \mid q_i, q'_j) - p_{\text{ent}}(a_i, a'_j \mid q_i, q'_j)|$ by bounding $\|\rho(i,j) - \rho\|_{\text{tr}}$, since the trace distance between two states is an upper bound on the variation distance of the probability distribution resulting from making any measurement on those two states.

The following technique was introduced by Ambainis et al. [3] and has been used extensively by Aaronson [1, 2].

CLAIM 20. *The trace distance between $\rho_{\text{AB}}(i,j)$ and ρ_{AB} is bounded by*

$$\|\rho_{\text{AB}}(i,j) - \rho_{\text{AB}}\|_{\text{tr}} \leq 6 \sum_{i'=1}^{i-1} \sqrt{1 - \pi_2(q_{i'})} + 6 \sum_{j'=1}^{j-1} \sqrt{1 - \pi_2(q_{j'})}.$$

Proof. By induction. The claim is clearly true for $(i,j) = (1,1)$. Given it is true for a particular value of (i,j), we show it is also true for $(i+1,j)$. In view of the symmetry, this is sufficient to establish the claim. We have

$$\begin{aligned}
&\|\rho_{\text{AB}}(i+1,j) - \rho_{\text{AB}}\|_{\text{tr}} \\
&\quad \leq \|\rho_{\text{AB}}(i+1,j) - \mathcal{W}_{q_i} \otimes \text{Id}\,(\rho_{\text{AB}})\|_{\text{tr}} + \|\mathcal{W}_{q_i} \otimes \text{Id}\,(\rho_{\text{AB}}) - \rho_{\text{AB}}\|_{\text{tr}} \\
&\quad \leq \|\mathcal{W}_{q_i} \otimes \text{Id}\ (\rho_{\text{AB}}(i,j) - \rho_{\text{AB}})\|_{\text{tr}} + 6\sqrt{1 - \pi_2(q_i)} \\
&\quad \leq \|\rho_{\text{AB}}(i,j) - \rho_{\text{AB}}\|_{\text{tr}} + 6\sqrt{1 - \pi_2(q_i)},
\end{aligned}$$

where we used the triangle inequality, Claim 19, and monotonicity of the trace distance. ∎

Putting everything together, it follows that

$$\begin{aligned}
\Delta(p_{\text{class}}, p_{\text{ent}}) &\leq \sum_{i,j=1}^{n} \pi(q_i, q'_j) \|\rho_{\text{AB}}(i,j) - \rho_{\text{AB}}\|_{\text{tr}} \\
&\leq 6 \sum_{i,j=1}^{n} \pi(q_i, q'_j) \left(\sum_{i'=1}^{i-1} \sqrt{1 - \pi_2(q_{i'})} + \sum_{j'=1}^{j-1} \sqrt{1 - \pi_2(q_{j'})} \right) \\
&= 12 \sum_{i=1}^{n} \sum_{i'=1}^{i-1} \pi(q_i) \sqrt{1 - \pi_2(q_{i'})} \\
&\leq 12|Q| \sum_{i'=1}^{n} \pi(q_{i'}) \sqrt{1 - \pi_2(q_{i'})} \\
&\leq 12|Q| \sqrt{1 - \pi_2} \\
&< 12|Q| \sqrt{\varepsilon},
\end{aligned}$$

since $\sqrt{1-x}$ is concave and $\pi_2 = \sum_q \pi(q)\pi_2(q) > 1 - \varepsilon$. ∎

5. Hardness of two-prover classical entangled games. In this section we prove our main theorem for two-prover classical entangled games. It shows that it is PSPACE-hard to decide, given a specification x for a succinct two-prover classical entangled game, whether its value is 1 or at most $1 - \varepsilon$ for $\varepsilon = \frac{1}{\text{poly}(|x|)}$. To state the result, we need some further definitions to clarify the notion of succinctly given games and state the connection between PSPACE and multiround single-prover games.

DEFINITION 21. *A language L is in* $\mathrm{MIP}^*_{c,s}(N,1)$ *if, for all x, there is a polynomial time (in $|x|$) mapping from x to classical N-prover one-round games $G_x = (\pi_x, V_x)$ such that it is possible to sample from π_x in polynomial time and compute the predicate V_x in polynomial time and the following are satisfied:*

(Completeness) *for all $x \in L$, the entangled value $\omega^*(G_x) \geq c(|x|)$, and*

(Soundness) *for all $x \notin L$, the entangled value $\omega^*(G_x) \leq s(|x|)$.*

Note that in this scenario the game is given *succinctly*: it is given by a description of V (as a polynomial time circuit, for instance, which implies that $|Q|$ and $|A|$ can be exponentially large in $|x|$) and a polynomial size description of π, which can be sampled in polynomial time. Hence the complexity parameter here is $|x|$, and $|Q|$ and $|A|$ can be exponential in $|x|$.

We also require the notion of single-prover games with multiple rounds. We modify our definition of a game (see section 2) to account for games with multiple rounds. Here we will consider only *nonadaptive* games: the probability distribution of questions in Q for each round k does not depend on the answers received in previous rounds, which is sufficient for PSPACE (see Theorem 22). However, we allow for the possibility that the questions asked in each round depend on the questions asked in previous rounds.[22] In other words a one-prover r-round game $G = (\pi_r, V_r)$ is given by a joint distribution $\pi_r \colon Q^r \to [0,1]$ and a predicate $V_r \colon A^r \times Q^r \to \{0,1\}$ (i.e., a function of all the questions and answers in all rounds according to which the verifier decides acceptance or rejection). The strategy is now a set of r functions W_k, where the kth function can depend on the previous questions and answers. The class $\mathrm{IP}_{c,s}(r)$ is given by Definition 21 when the game is a single-prover multiround game with r rounds, and the class $\mathrm{IP}_{c,s}$ is the union of $\mathrm{IP}_{c,s}(r)$ for all polynomial r.

THEOREM 22 (see [35, 39]). *For any constant $s_3 < 1$, $\mathrm{IP}_{1,s_3} = \mathrm{PSPACE}$. Moreover, there are "public-coin" (and thus nonadaptive) single-prover interactive proofs for* PSPACE*; i.e., in each round the distribution of the questions is uniform and independent of the answers of the prover and of other rounds* [15, 40].

Hereafter we fix the constant $s_3 < 1$ arbitrarily. With these notions in place we can state our main result for two-prover classical entangled games.

THEOREM 23. $\mathrm{PSPACE} \subseteq \bigcup_{p\colon \text{polynomial}} \mathrm{MIP}^*(2,1)_{1,1-1/p}$.

We note that if a parallel repetition theorem could be established for two-prover classical entangled games, then the containment in Theorem 23 could be improved to $\mathrm{PSPACE} \subseteq \mathrm{MIP}^*(2,1)_{1,s}$ with constant or even exponentially small s. Note that the inclusion $\mathrm{PSPACE} \subseteq \mathrm{MIP}^*(2,1)_{1,s}$ was very recently proved by Ito, Kobayashi, and Matsumoto [21], even for exponentially small s. Their proof shows that the two-prover one-round system for PSPACE that we use in the proof of Lemma 24 remains sound even against *nonsignaling* provers and then uses a previously known parallel repetition theorem for nonsignaling provers [19]. The parallel repetition question remains open for *entangled* provers: this is a particularly interesting direction to pursue, in light of the perfect parallel repetition theorem for entangled XOR games of Cleve et al. [12] (which uses the SDP description on the value of these games).

To prove Theorem 23 we use the PSPACE-characterization in Theorem 22 and show the following.

LEMMA 24. *There is a constant $s_4 > 0$ such that for every succinctly given single-prover r-round nonadaptive game $G = (\pi_r, V_r)$, of value $\omega(G)$ with question set Q and answer set A, there is a two-prover one-round classical game $G' = (\pi, V)$*

[22] Note that this is equivalent to having a joint distribution of the questions, where we obtain the distribution on the ith question as the corresponding marginal.

with question set Q^r and answer set A^r with entangled value $\omega^*(G') \geq \omega(G)$ such that if $\omega^*(G') > 1 - \varepsilon$, then $\omega(G) > s_3$ for $\varepsilon = \frac{s_4}{r^2}$. Moreover, a succinct description of G' can be computed from a description of G in polynomial time, and G' is such that sampling π and computing V can be done in polynomial time.

Lemma 24 shows $\mathrm{IP}(r)_{1,s_3} \subseteq \mathrm{MIP}(2,1)^*_{1,1-\frac{s_4}{r^2}}$. Combined with Theorem 22, this gives Theorem 23.

The rest of this section is dedicated to the proof of Lemma 24. It follows the main traits of the proofs of the previous two hardness results. Our construction of the two-prover one-round game uses a protocol of [9] which was used there to prove that PSPACE has two-prover one-round classical proof systems. We show that this protocol remains sound even against entangled provers, albeit with larger soundness. To prove this we again use the consistency test with the extra prover to extract almost-commuting conditions on the operators of the provers. This allows us to round in a similar fashion from a good strategy for the entangled game to a strategy for the single-prover game which succeeds with relatively large probability.

The modified two-prover game. In the constructed game G', the verifier samples a series of questions $q_1, \ldots, q_r$ according to the distribution $\pi_r(q_1, \ldots, q_r)$. He picks k uniformly at random in $\{1, \ldots, r\}$ and sends questions $q_1, \ldots, q_r$ to Alice and $q_1, \ldots, q_k$ to Bob. He receives answers $a_1, \ldots, a_r$ from Alice and $a'_1, \ldots, a'_k$ from Bob. He accepts iff the following are both true.

Classical Test. The answers Alice gives would win the game G; i.e., the answers $a_1, \ldots, a_r$ satisfy $V(a_1, \ldots, a_r \mid q_1, \ldots, q_r) = 1$.

Consistency Test. For all i in $\{1, \ldots, k\}$, $a_i = a'_i$.

It is again obvious that the value of the new game is lower bounded by the value of the original game: if both provers reply according to an optimal classical strategy for the original r-round game, then they will always give consistent answers, so their acceptance probability is exactly $\omega(G)$.

It is also easy to see that the constructed game has the same complexity as the original game. The new verifier essentially implements the original verifier and the consistency test, which can be described in linear time in $r \log |A|$. The sampling procedure also has the same complexity as sampling from the original π_r. Obviously it is possible to compute the description of the new game from that of the original game in polynomial time.

To prove Lemma 24 we need to show the following result for $\varepsilon = \frac{s_4}{r^2}$, where s_4 is some sufficiently small constant.

LEMMA 25. *If $\omega^*(G') > 1 - \varepsilon$, then $\omega(G) > s_3$.*

Proof. Consider an entangled strategy for G' that succeeds with probability greater than $1 - \varepsilon$.[23] For any sequence of questions $\boldsymbol{q} = (q_1, \ldots, q_r)$ we define $\boldsymbol{q}_k$ to be the sequence $(q_1, \ldots, q_k)$. Similarly, for any sequence $\boldsymbol{a} = (a_1, \ldots, a_r)$ of possible answers we will denote its prefix $(a_1, \ldots, a_k)$ by $\boldsymbol{a}_k$. Note that, when we write $\boldsymbol{a}_k$ and $\boldsymbol{a}_l$ for some $1 \leq k, l \leq r$, we refer to prefixes of the *same* sequence $\boldsymbol{a} = (a_1, \ldots, a_r)$, whereas we will write $\boldsymbol{a}_k$ and $\boldsymbol{a}'_l$ if we refer to *different* sequences $\boldsymbol{a}$ and $\boldsymbol{a}'$.

Let $|\Psi\rangle$ be the entangled state shared by Alice and Bob and define a corresponding density matrix $\rho = |\Psi\rangle\langle\Psi|$. Let $\tilde{\mathcal{W}}_{\boldsymbol{q}_r} = \{\tilde{W}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\}$ and $\mathcal{W}_{\boldsymbol{q}_k} = \{W^{\boldsymbol{a}'_k}_{\boldsymbol{q}_k}\}$ be the measurements that they perform when asked questions $\boldsymbol{q}_r$ (resp., $\boldsymbol{q}_k$) giving answers $\boldsymbol{a}_r$ (resp., $\boldsymbol{a}'_k$). As in section 4 we can assume that these measurements are projective.

[23] Again, as in subsection 3.2, we in fact consider a strategy with finite entanglement that has success probability greater than $1 - \varepsilon - \delta$ for some $\delta = O(\varepsilon)$, which we will not write.

The provers pass the consistency test with probability $\pi_2 = \frac{1}{r}\sum_{k=1}^{r}\pi_2(k)$, where

$$\pi_2(k) = \mathrm{E}_{\boldsymbol{q}_r}\left[\sum_{\boldsymbol{a}_r}\mathrm{Tr}\big(\tilde{W}_{\boldsymbol{q}_r}^{\boldsymbol{a}_r}\otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}\rho\big)\right]$$

is the probability that the two provers give consistent answers when the verifier has picked k as the separation point. Conditioned on the fact that they give consistent answers, they succeed in the classical test with probability $\pi_1 = \frac{1}{r}\sum_{k=1}^{r}\pi_1(k)$, where

$$\pi_1(k) = \mathrm{E}_{\boldsymbol{q}_r}\left[\sum_{\boldsymbol{a}_r} p_{\mathrm{ent}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r, k)V(\boldsymbol{a}_r \mid \boldsymbol{q}_r)\right],$$

and $p_{\mathrm{ent}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r, k) = \mathrm{Tr}\big(\tilde{W}_{\boldsymbol{q}_r}^{\boldsymbol{a}_r}\otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}\rho\big)$ is the probability that Alice answers $\boldsymbol{a}_r$ and Bob answers consistently, given that the verifier picked index k.

Rounding to a classical strategy. Given a strategy for the constructed classical entangled game G', we define a strategy for the classical prover of the original game G in the following way. In round k, given the questions to the prover so far are $\boldsymbol{q}_k$ and the prover gives answers $\boldsymbol{a}_{k-1}$, he answers a_k to question q_k with probability

$$p_{\mathrm{class}}(a_k \mid \boldsymbol{q}_k, \boldsymbol{a}_{k-1}) = \frac{\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}W_{\boldsymbol{q}_{k-1}}^{\boldsymbol{a}_{k-1}}\cdots W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)}{\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_{k-1}}^{\boldsymbol{a}_{k-1}}\cdots W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)}$$

(recall that all $\boldsymbol{a}_k, \boldsymbol{a}_{k-1}, \ldots, \boldsymbol{a}_1$ refer to prefixes of the same sequence). Note that $\sum_{a_k} p_{\mathrm{class}}(a_k \mid \boldsymbol{q}_k, \boldsymbol{a}_{k-1})$ could be less than 1 (we will see from its operational definition that it is always bounded by 1). To complete it to a probability distribution we add a special symbol "abort" that the prover can send in any round, making him lose the game.[24]

This probability distribution has the following interpretation. For any operator X, denote $X(\rho) = X\rho X^\dagger$. In the first round the prover in the classical game receives a question q_1, and applies the measurement $\mathcal{W}_{\boldsymbol{q}_1}$ on Bob's part of ρ, answering a_1 with probability $\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big) = p_{\mathrm{class}}(a_1 \mid \boldsymbol{q}_1)$. He is then left with the state $\frac{\mathrm{Id}\otimes W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}(\rho)}{\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)}$. Upon receiving a question q_2 in the second round, he measures this state with $\mathcal{W}_{\boldsymbol{q}_2}$, answering a_2 with probability $\frac{\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_2}^{\boldsymbol{a}_2}W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)}{\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)} = p_{\mathrm{class}}(a_2 \mid \boldsymbol{q}_2, \boldsymbol{a}_1)$ if as a result of his measurement he obtains a sequence $\boldsymbol{a}_2 = (a_1, a_2)$ consistent with the a_1 he had measured in the first round and an abort symbol in case the sequence he measures has an $a_1' \neq a_1$. The resulting state in case of nonabortion is $\frac{\mathrm{Id}\otimes W_{\boldsymbol{q}_2}^{\boldsymbol{a}_2}W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}(\rho)}{p_{\mathrm{class}}(a_2|\boldsymbol{q}_2,\boldsymbol{a}_1)\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)} = \frac{\mathrm{Id}\otimes W_{\boldsymbol{q}_2}^{\boldsymbol{a}_2}W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}(\rho)}{\mathrm{Tr}\big(\mathrm{Id}\otimes W_{\boldsymbol{q}_2}^{\boldsymbol{a}_2}W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1}\rho\big)}$. The prover proceeds similarly in the subsequent rounds. In other words, the prover sequentially performs all the measurements $\mathcal{W}_{\boldsymbol{q}_k}$, and answers according to the resulting distribution, aborting in case the answers he measures in round k contradict the answers that he has already given in previous rounds.

What is the probability that a fixed sequence of answers $\boldsymbol{a}_r$ is given by the prover? We have that $p_{\mathrm{class}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r) = p_{\mathrm{class}}(a_r \mid \boldsymbol{q}_r, \boldsymbol{a}_{r-1})\cdots p_{\mathrm{class}}(a_2 \mid \boldsymbol{q}_2, \boldsymbol{a}_1)\cdot p_{\mathrm{class}}(a_1 \mid \boldsymbol{q}_1)$.

[24] Technically speaking the extra symbol makes it a different game. We could also have the prover send a random answer whenever sampling from the complement of the distribution. This can at most increase the prover's winning probability, so both games have winning probability bounded by $\omega(G)$.

Because of cancellation, we obtain

$$p_{\text{class}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r) = \operatorname{Tr}\big(\mathrm{Id} \otimes W_{\boldsymbol{q}_r}^{\boldsymbol{a}_r} \cdots W_{\boldsymbol{q}_1}^{\boldsymbol{a}_1} \rho\big).$$

We will show that this classical strategy is a good one by relating $p_{\text{class}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r)$ to $p_{\text{ent}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r, r)$ as per the following lemma.

LEMMA 26. *The (weighted) statistical distance between p_{class} and p_{ent} is*

$$\Delta(p_{\text{class}}, p_{\text{ent}}) = \mathrm{E}_{\boldsymbol{q}_r}\left[\sum_{\boldsymbol{a}_r} \left|p_{\text{class}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r) - p_{\text{ent}}(\boldsymbol{a}_r \mid \boldsymbol{q}_r, r)\right|\right] < 7r\sqrt{\varepsilon}.$$

This lemma is the analogue of Lemmas 14 and 17, and its proof is very similar. Before proceeding, we first show how it implies Lemma 25. For the total acceptance probability of the entangled provers we have $1 - \varepsilon < 1/r \sum_{k=1}^{r} \min(\pi_1(k), \pi_2(k))$ because for any index k that is picked by the verifier we require the provers to succeed in both the classical test and the consistency test. This implies that $\pi_2(r) > 1 - r\varepsilon$, so Bob's answers can be used to give correct answers to the classical test with probability greater than $1 - r\varepsilon$, and by Lemma 26 this implies that the classical test has success probability greater than $1 - r\varepsilon - 7r\sqrt{\varepsilon}$. For $\varepsilon = \frac{s_4}{r^2}$ for a sufficiently small constant s_4, this is more than s_3, which implies Lemma 25. □

Proof of Lemma 26. As in the case of three-prover classical entangled games, the fact that Alice's and Bob's answers must be consistent means that Alice's answers can be used to predict Bob's, and thus Bob cannot use his share of the entanglement too much if they are to succeed in the consistency test. This means that the action of Bob's operators $\mathcal{W}$ on the entangled state ρ is close to the identity, at least when Alice applies the corresponding $\tilde{\mathcal{W}}$ on her share of ρ. The following claim makes this explicit and will be used to relate the classical and entangled strategies.

CLAIM 27. *Let the projector $\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} = \sum_{a_{k+1},\ldots,a_r} \tilde{W}_{\boldsymbol{q}_r}^{\boldsymbol{a}_r}$. The following hold for every $k \in \{1, \ldots, r\}$:*

$$\mathrm{E}_{\boldsymbol{q}_r}\left[\sum_{\boldsymbol{a}_k} \left\|\mathrm{Id} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho) - \tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)\right\|_{\text{tr}}\right] \le 3\sqrt{1 - \pi_2(k)}, \tag{7}$$

$$\mathrm{E}_{\boldsymbol{q}_r}\left[\sum_{\boldsymbol{a}_k} \left\|\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes \mathrm{Id}\,(\rho) - \tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)\right\|_{\text{tr}}\right] \le 3\sqrt{1 - \pi_2(k)}, \tag{8}$$

$$\mathrm{E}_{\boldsymbol{q}_r}\left[\sum_{\boldsymbol{a}_k} \left\|\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_{k-1}} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho) - \tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)\right\|_{\text{tr}}\right] \le 1 - \pi_2(k). \tag{9}$$

Proof. Inequalities (7) and (8) are a direct application of Lemma 18, combined with the definition of $\pi_2(k)$. To prove inequality (9), note that, since $\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_{k-1}} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho) \ge \tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)$, we have that

$$\begin{aligned}
&\left\|\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_{k-1}} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho) - \tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)\right\|_{\text{tr}} \\
&\quad = \operatorname{Tr}\big(\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_{k-1}} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)\big) - \operatorname{Tr}\big(\tilde{V}_{\boldsymbol{q}_r}^{\boldsymbol{a}_k} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k}(\rho)\big) \\
&\quad = \sum_{a'_k \neq a_k, a'_{k+1}, \ldots, a'_r} \operatorname{Tr}\big(\tilde{W}_{\boldsymbol{q}_r}^{(\boldsymbol{a}_{k-1}, a'_k, \ldots, a'_r)} \otimes W_{\boldsymbol{q}_k}^{\boldsymbol{a}_k} \rho\big).
\end{aligned}$$

Since $\sum_{\boldsymbol{a}_r,\boldsymbol{a}'_k} \mathrm{Tr}(\tilde{W}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r} \otimes W^{\boldsymbol{a}'_k}_{\boldsymbol{q}_k}\rho) = 1$,

$$\begin{aligned} 1-\pi_2(k) &= \mathrm{E}_{\boldsymbol{q}_r}\Bigg[\sum_{\boldsymbol{a}_r,\boldsymbol{a}'_k\neq \boldsymbol{a}_k} \mathrm{Tr}\big(\tilde{W}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r} \otimes W^{\boldsymbol{a}'_k}_{\boldsymbol{q}_k}\rho\big)\Bigg] \\ &\geq \mathrm{E}_{\boldsymbol{q}_r}\Bigg[\sum_{\boldsymbol{a}_r,a'_k\neq a_k} \mathrm{Tr}\big(\tilde{W}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r} \otimes W^{(\boldsymbol{a}_{k-1},a'_k)}_{\boldsymbol{q}_k}\rho\big)\Bigg], \end{aligned}$$

which completes the proof. □

Observe that, for any set of orthogonal projectors $\{W^a\}$ and for any two matrices σ_1 and σ_2, we have that $\sum_a \|W^a\sigma_1 W^a - W^a\sigma_2 W^a\|_{\mathrm{tr}} \leq \|\sigma_1-\sigma_2\|_{\mathrm{tr}}$. Using this successively for the sets $\{W^{\boldsymbol{a}_2}_{\boldsymbol{q}_2}\}_{\boldsymbol{a}_2}$, …, $\{W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\}_{\boldsymbol{a}_r}$, from inequality (7) with $k=1$ we get

$$\mathrm{E}_{\boldsymbol{q}_r}\Bigg[\sum_{\boldsymbol{a}_r} \big\|\mathrm{Id}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_1}_{\boldsymbol{q}_1}(\rho) - \tilde{V}^{\boldsymbol{a}_1}_{\boldsymbol{q}_r}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_1}_{\boldsymbol{q}_1}(\rho)\big\|_{\mathrm{tr}}\Bigg] \leq 3\sqrt{1-\pi_2(1)}.$$

Similarly, from inequality (8),

$$\mathrm{E}_{\boldsymbol{q}_r}\Bigg[\sum_{\boldsymbol{a}_r} \big\|\tilde{V}^{\boldsymbol{a}_1}_{\boldsymbol{q}_r}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_1}_{\boldsymbol{q}_1}(\rho) - \tilde{V}^{\boldsymbol{a}_1}_{\boldsymbol{q}_r}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_2}_{\boldsymbol{q}_2}(\rho)\big\|_{\mathrm{tr}}\Bigg] \leq 3\sqrt{1-\pi_2(1)},$$

and from inequality (9) with $k=2$ we get

$$\mathrm{E}_{\boldsymbol{q}_r}\Bigg[\sum_{\boldsymbol{a}_r} \big\|\tilde{V}^{\boldsymbol{a}_1}_{\boldsymbol{q}_r}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_2}_{\boldsymbol{q}_2}(\rho) - \tilde{V}^{\boldsymbol{a}_2}_{\boldsymbol{q}_r}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_2}_{\boldsymbol{q}_2}(\rho)\big\|_{\mathrm{tr}}\Bigg] \leq 1-\pi_2(2).$$

Repeating these operations for each k, adding the equations, and using the triangle inequality and the concavity of the function $\sqrt{1-x}$, we finally have

$$\begin{aligned} &\mathrm{E}_{\boldsymbol{q}_r}\Bigg[\sum_{\boldsymbol{a}_r} \big\|\mathrm{Id}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\cdots W^{\boldsymbol{a}_1}_{\boldsymbol{q}_1}(\rho) - \tilde{V}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}\otimes W^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}(\rho)\big\|_{\mathrm{tr}}\Bigg] \\ &\qquad \leq 6\sum_{k=1}^{r-1}\sqrt{1-\pi_2(k)} + \sum_{k=2}^{r}(1-\pi_2(k)) \leq 7r\sqrt{1-\pi_2}. \end{aligned}$$

Since $\tilde{V}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r} = \tilde{W}^{\boldsymbol{a}_r}_{\boldsymbol{q}_r}$, the lemma follows because the trace distance is an upper bound on the variation distance of the probability distribution resulting from making any measurement on these two states. □

6. Conclusions and open questions. We have established that it is NP-hard to approximate the value of both two-prover quantum entangled games and three-prover classical entangled games. The most immediate question is whether we can improve the inapproximability ratio to better than an inverse polynomial in the number of questions. Are there additional tests that further limit the advantage provers can obtain by sharing entanglement?

Interestingly, very recently [21] described an example, based on the Magic Square game, showing that the inverse-polynomial gap *is* achievable if one does not place any restrictions on the structure of the original game under consideration. However, this example applies only to the *two-prover* setting, and not to the three-prover case,

due to a subtle difference on the new question's distribution between those two cases; this leaves open the possibility that more than two provers could be more useful. In fact, it is known that if there are as many provers as there are questions, then sharing entanglement does not help, even if the verifier talks only to two provers chosen at random.[25] However, no separations are known between models with a constant (larger than 1) number of provers.

In a very recent work [24] a subset of the authors obtains parallelization results for the case of quantum multiround entangled games, showing that any such game with k provers and r rounds can be parallelized to a three-turn game with k provers at the expense of a poly(r) factor in the value of the game. Moreover, such a game can be parallelized to two turns, or one round, by adding a $(k+1)$st prover. We do not know whether it is possible to parallelize quantum entangled games from three to two turns without adding an additional prover.

A related question is whether *parallel repetition* is possible. This is particularly interesting in light of the perfect parallel repetition theorem for entangled XOR games of Cleve et al. [12] and the parallel repetition result for entangled unique games of Kempe, Regev, and Toner [26][26] (which both use the SDP description or relaxation of the value of these games). No parallel repetition result is known for general entangled games.

There are a number of other important questions that our work does not address. Can we prove *upper* bounds on the hardness of computing the value of entangled games? It is instructive here to compare to the case where the provers share nonsignaling correlations, where there is an efficient linear-programming algorithm to compute the value of a game [38, 20].[27] In the entangled-prover case, it is still not known whether the decision problem corresponding to finding the value of an entangled-prover game is recursive! The issue is that we are not currently able to prove any bounds on the amount of entanglement required to play a game optimally, even approximately.

Acknowledgments. We thank Tsuyoshi Ito, Jaikumar Radhakrishnan, Oded Regev, Amnon Ta-Shma, Mario Szegedy, and Andy Yao for helpful discussions and John Watrous for pointing out that the optimal quantum value of a game might not be achievable with finite-dimensional entanglement.

REFERENCES

[1] S. Aaronson, *Limitations of quantum advice and one-way communication*, Theory Comput., 1 (2005), pp. 1–28.

[2] S. Aaronson, QMA/qpoly $\subseteq$ PSPACE/poly*: De-Merlinizing quantum protocols*, in Proceedings of the Twenty-First Annual IEEE Conference on Computational Complexity, 2006, pp. 261–273.

[3] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, *Dense quantum coding and quantum finite automata*, J. ACM, 49 (2002), pp. 496–511.

[4] P. K. Aravind, *A Simple Demonstration of Bell's Theorem Involving Two Observers and No Probabilities or Inequalities*, http://arxiv.org/abs/quant-ph/020670 (2003).

[25] A proof of this fact follows from Theorem 2 of [41] (see also [46]).

[26] See also [25] for a recent result that perfect parallel repetition does not hold in general for entangled games.

[27] The reason that our proof does not work for nonsignaling provers is that there is no notion of a partial measurement of a nonsignaling probability distribution, and thus the classical strategy we use in our proofs cannot be defined.

[5] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, *Proof verification and the hardness of approximation problems*, J. ACM, 45 (1998), pp. 501–555.
[6] S. Arora and S. Safra, *Probabilistic checking of proofs: A new characterization of* NP, J. ACM, 45 (1998), pp. 70–122.
[7] J. S. Bell, *On the Einstein Podolsky Rosen paradox*, Physics, 1 (1964), pp. 195–200.
[8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, *Quantum fingerprinting*, Phys. Rev. Lett., 87 (2001), article 167902.
[9] J.-Y. Cai, A. Condon, and R. J. Lipton, PSPACE *is provable by two provers in one round*, J. Comput. System Sci., 48 (1994), pp. 183–193.
[10] R. Cleve, D. Gavinsky, and R. Jain, *Entanglement-resistant two-prover interactive proof systems and non-adaptive PIRs*, Quantum Inf. Comput., 9 (2009), pp. 648–656.
[11] R. Cleve, P. Høyer, B. Toner, and J. Watrous, *Consequences and limits of nonlocal strategies*, in Proceedings of the Nineteenth Annual IEEE Conference on Computational Complexity, 2004, pp. 236–249.
[12] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay, *Perfect parallel repetition theorem for quantum XOR proof systems*, Comput. Complexity, 17 (2008), pp. 282–299.
[13] K. R. Davidson and S. J. Szarek, *Local operator theory, random matrices and Banach spaces*, in Handbook of the Geometry of Banach Spaces, Vol. 1, W. B. Johnson and J. Lindenstrauss, eds., North–Holland, Amsterdam, 2001, pp. 317–366.
[14] R. Exel and T. Loring, *Almost commuting unitary matrices*, Proc. Amer. Math. Soc., 106 (1989), pp. 913–915.
[15] S. Goldwasser and M. Sipser, *Private coins versus public coins in interactive proof systems*, in Randomness and Computation, Adv. Comput. Res. 5, S. Micali, ed., JAI Press, Greenwich, CT, 1989, pp. 73–90.
[16] G. Gutoski and J. Watrous, *Toward a general theory of quantum games*, in Proceedings of the 39th Annual ACM Symposium on Theory of Computing, 2007, pp. 565–574.
[17] P. Halmos, *Some unknown problems of unknown depth about operators on Hilbert space*, Proc. Roy. Soc. Edinburgh Sect. A, 76 (1976/77), pp. 67–76.
[18] J. Håstad, *Some optimal inapproximability results*, J. ACM, 48 (2001), pp. 798–859.
[19] T. Holenstein, *Parallel repetition: Simplifications and the no-signaling case (extended abstract)*, in Proceedings of the 39th Annual ACM Symposium on Theory of Computing, 2007, pp. 411–419.
[20] T. Ito, *Polynomial-space approximation of no-signaling provers*, in Proceedings of the 37th International Colloquium on Automata, Languages and Programming, Springer-Verlag, Berlin, 2010, pp. 140–151.
[21] T. Ito, H. Kobayashi, and K. Matsumoto, *Oracularization and two-prover one-round interactive proofs against nonlocal strategies*, in Proceedings of the Twenty-Fourth Annual IEEE Conference on Computational Complexity, 2009, pp. 217–228.
[22] T. Ito, H. Kobayashi, D. Preda, X. Sun, and A. C.-C. Yao, *Generalized Tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems*, in Proceedings of the Twenty-Third Annual IEEE Conference on Computational Complexity, 2008, pp. 187–198.
[23] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous, QIP = PSPACE, in Proceedings of the 42nd Annual ACM Symposium on Theory of Computing, 2010, pp. 573–582.
[24] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick, *Using entanglement in quantum multi-prover interactive proofs*, Comput. Complexity, 18 (2009), pp. 273–307.
[25] J. Kempe and O. Regev, *No strong parallel repetition with entangled and non-signaling provers*, in Proceedings of the Twenty-Fifth Annual IEEE Conference on Computational Complexity, 2010, pp. 7–15.
[26] J. Kempe, O. Regev, and B. Toner, *Unique games with entangled provers are easy*, in Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science, 2008, pp. 457–466.
[27] J. Kempe and T. Vidick, *On the Power of Entangled Quantum Provers*, http://arxiv.org/abs/quant-ph/0612063 (2006).
[28] A. Kitaev and J. Watrous, *Parallelization, amplification, and exponential time simulation of quantum interactive proof systems*, in Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, 2000, pp. 608–617.
[29] A. Yu. Kitaev, *Quantum coin-flipping*, talk at the 6th Workshop on Quantum Information Processing, Mathematical Science Research Institute, Berkeley, CA, 2002.
[30] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Grad. Stud. Math. 47, American Mathematical Society, Providence, RI, 2002.

[31] H. Kobayashi and K. Matsumoto, *Quantum multi-prover interactive proof systems with limited prior entanglement*, J. Comput. System Sci., 66 (2003), pp. 429–450.
[32] H. Kobayashi, K. Matsumoto, and T. Yamakami, *Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur?*, Chic. J. Theoret. Comput. Sci., 2009 (2009), article 3.
[33] D. Leung, B. Toner, and J. Watrous, *Coherent State Exchange in Multi-prover Quantum Interactive Proof Systems*, http://arxiv.org/abs/0804.4188 (2008).
[34] H. Lin, *Almost commuting selfadjoint matrices and applications*, in Operator Algebra and Their Applications, Fields Inst. Commun. 13, P. A. Fillmore and J. A. Mingo, eds., American Mathematical Society, Providence, RI, 1997, pp. 193–233.
[35] C. Lund, L. Fortnow, H. Karloff, and N. Nisan, *Algebraic methods for interactive proof systems*, J. Assoc. Comput. Mach., 39 (1992), pp. 859–868.
[36] M. Navascués, S. Pironio, and A. Acín, *Bounding the set of quantum correlations*, Phys. Rev. Lett., 98 (2007), article 010401.
[37] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2000.
[38] D. Preda, *private communication*.
[39] A. Shamir, IP = PSPACE, J. Assoc. Comput. Mach., 39 (1992), pp. 869–877.
[40] A. Shen, IP = PSPACE*: Simplified proof*, J. Assoc. Comput. Mach., 39 (1992), pp. 878–880.
[41] B. M. Terhal, A. C. Doherty, and D. Schwab, *Symmetric extensions of quantum states and local hidden variable theories*, Phys. Rev. Lett., 90 (2003), article 157903.
[42] B. Toner, *Monogamy of non-local quantum correlations*, Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci., 465 (2009), pp. 59–69.
[43] B. S. Tsirelson, *Quantum analogues of the Bell inequalities. The case of two spacially separated domains*, J. Soviet Math., 36 (1987), pp. 557–570.
[44] D. Voiculescu, *Remarks on the singular extension in the C^*-algebra of the Heisenberg group*, J. Operator Theory, 5 (1981), pp. 147–170.
[45] D. Voiculescu, *Asymptotically commuting finite rank unitary operators without commuting approximants*, Acta Sci. Math. (Szeged), 45 (1983), pp. 429–431.
[46] R. F. Werner, *An application of Bell's inequalities to a quantum state extension problem*, Lett. Math. Phys., 17 (1989), pp. 359–363.
[47] A. Winter, *Coding Theorems of Quantum Information Theory*, Ph.D. thesis, Fakultät für Mathematik, Universität Bielefeld, Bielefeld, Germany, 1999.
[48] A. C.-C. Yao, *private communication*, 2007.